

Vollständige Bell-Zustandsanalyse

für superdichtes Quantenkodieren

Diplomarbeit an der Fakultät für Physik
der
Ludwig-Maximilians-Universität München
Arbeitsgruppe Prof. Dr. Harald Weinfurter

Gerhard Huber

9. August 2004

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Axel Schenzle

Inhaltsverzeichnis

1	Einleitung	5
2	Theoretische Grundlagen	7
2.1	Klassische Informationstheorie	7
2.1.1	Einführung	7
2.1.2	Ein einfaches Kommunikationsmodell	8
2.1.3	Informationsgehalt und Entropie	9
2.1.4	Gegenseitige Information	13
2.1.5	Die Kanalkapazität	15
2.2	Quanteninformationstheorie	16
2.2.1	Quantales Zweiniveausystem	17
2.2.2	Die von Neumann-Entropie	22
2.2.3	Die Messung	23
2.2.4	Verschränkung	28
3	Superdichtes Quantenkodieren	34
3.1	Einführung	34
3.2	Das Protokoll	34
3.2.1	Ablauf	34
3.2.2	Erläuterungen	36
3.2.3	Informationsübertragung beim Dense Coding	37
3.3	Einteilchenstatistik der Bell-Zustände	38
3.3.1	Reduzierte Dichteoperatoren	38
3.3.2	Lokale Messungen	39
3.4	Diskussion	40
4	Erzeugung der verschränkten Zustände	42
4.1	Einführung	42
4.2	Spontane parametrischen Fluoreszenz	43
4.2.1	Theorie der Konversion	43
4.2.2	Räumliche Verteilung der Emissionsmoden	44
4.2.3	Die Photonenpaarquelle	45
4.3	Zur Detektion der Einzelphotonen	49

4.4	Die Spektren der Einzelphotonen	51
4.5	Die Polarisationsverschränkung	53
4.5.1	Transformation des Quellenzustands	53
4.5.2	Die Polarisationskorrelationen	54
5	Vollständige Bell-Zustandsanalyse	58
5.1	Einleitung	58
5.2	Unterscheidbarkeit der Bell-Zustände	59
5.3	Das CNOT Gatter	61
5.3.1	Vollständige Gattersysteme	61
5.3.2	Das CNOT als maximal verschränkendes Gatter	62
5.4	Verschränkung in mehreren Freiheitsgraden	63
5.5	Implementierung	65
5.5.1	HOM-Interferenz	67
5.5.2	Das asymmetrische Interferometer	71
5.5.3	Analyse in P/M-Basis	73
5.5.4	Die Detektoreinheit	76
5.5.5	Die Koinzidenzeinheit	80
5.6	Ergebnisse	83
6	Zusammenfassung und Ausblick	88
A	Anhang	90
A.1	Fit-Funktionen und Kontrast	90
A.2	Wellenplättchen-Matrizen	90
A.3	Stabilisierung des Interferometers	91
A.4	Die Detektoreinheit	93
	Literaturverzeichnis	95

1 Einleitung

Das noch recht junge Gebiet der Quanteninformation beschäftigt sich mit der Frage, welchen Einfluss nichtklassische Eigenschaften quantaler Objekte auf die Art und Weise haben, in der Information in ihnen kodiert wird. Diese Quantenobjekte können zum Beispiel einzelne Atome, Ionen oder Photonen sein. Die Information wird in den Freiheitsgraden des Systems kodiert, also zum Beispiel in der Polarisierung einzelner Photonen, wie es auch in der vorliegenden Arbeit geschieht.

Betrachtet man Systeme aus mehreren Quantenobjekten, so gibt es nach dem in der Quantenmechanik fundamentalen Superpositionsprinzip bestimmte Zustände, deren Eigenschaften in starkem Gegensatz zur klassischen Beschreibung der Natur stehen.

Diese Zustände heißen "verschränkt". Sie zeichnen sich unter anderem dadurch aus, dass sie nicht vollständig durch die Eigenschaften der einzelnen Quantenobjekte, die das Gesamtsystem bilden, beschrieben werden können.

Insbesondere waren es die wechselseitigen Eigenschaften (Korrelationen) in verschränkten Zweiteilchensystemen, die schon EINSTEIN, PODOLSKI und ROSEN 1935 dazu brachten, die Vollständigkeit der quantenmechanischen Beschreibung der Natur in Zweifel zu ziehen [1].

Aus heutiger Sicht der Quanteninformationstheorie sind es gerade die verschränkten Zustände, die es uns erlauben, Information in klassisch nicht vorstellbarer Art zu kodieren und zu übertragen. Dabei gibt es so genannte maximal verschränkte Zustände, bei denen die nichtklassischen Eigenschaften am deutlichsten zu Tage treten.

In den meisten Experimenten, die sich die Verschränkung zweier Quantenobjekte zunutze machen, um Information nichtklassisch zu übertragen, ist die Messung in der so genannten Bell-Basis nötig. Sie ist eine Basis aus maximal verschränkten Zweiteilchenzuständen, den Bell-Zuständen. Ohne eine solche Messung, beziehungsweise Projektion, kann man die Ressource der Verschränkung in den Systemen nicht ausnützen.

Beispiele hierfür sind etwa das Teleportieren[2] oder das superdichte Quantenkodieren [3], welches ich in dieser Arbeit durchführen werde.

Die Messung in der Bell-Basis ist in diesen (und vielen anderen) Protokollen zur Verschränkung unabdingbare Voraussetzung für das Auftreten der nichtklassischen Phänomene. Speziell im Falle des superdichten Quantenkodierens ist es nötig, dass die Informa-

tion, die von einer Partei (A) in ein quantales System kodiert worden ist, indem sie einen der vier Bell-Zustände präpariert, von einer anderen Partei (B) ausgelesen werden kann. Dazu müssen von B die vier Zustände unterschieden werden können. Diese Aufgabe nennt man auch Bell-Zustandsanalyse oder Bell-Zustandsunterscheidung. Wenn nicht alle vier Bell-Zustände unterschieden werden können, kann B auch nicht die gesamte Information aus dem System extrahieren.

Es wurde jedoch gezeigt, dass die vier Bell-Zustände mit passiven linearoptischen Mitteln (dazu gehören alle "üblichen" optischen Elemente wie Strahlteiler und Phasenschieber) nicht perfekt unterschieden werden können [4]. Tatsächlich kann man maximal zwei der vier Zustände mit Sicherheit unterscheiden.

Wie wir genau sehen werden, kann die Wirkung der Bell-Zustandsanalyse durch ein CNOT-Gatter beschrieben werden. Die experimentelle Realisierung eines solchen Gatters würde einen Schritt hin zu vernetzten Gatter-"Schaltungen" in einem Quantencomputer bedeuten, da das CNOT-Gatter zusammen mit anderen, leicht realisierbaren, Gattern durch Vernetzung die Durchführung jeder unitären Berechnung ermöglicht.

Um die vollständige Bell-Zustandsanalyse durchführen zu können, folge ich in dieser Arbeit einem Vorschlag von KWIAT und WEINFURTER [5], und mache Gebrauch von der zusätzlichen Energie-Zeit Verschränkung der maximal polarisationsverschränkten Photonenpaare aus spontaner parametrischer Fluoreszenz. Man kann die Bell-Zustände somit in einem höherdimensionalen Hilbertraum analysieren und umgeht somit die Beschränkungen durch linearoptische Elemente.

Dadurch wird es mir möglich sein, *alle vier* Bell-Zustände unterscheiden zu können und somit optimales superdichtes Quantenkodieren zu präsentieren.

2 Theoretische Grundlagen

Inhalt

2.1	Klassische Informationstheorie	7
2.1.1	Einführung	7
2.1.2	Ein einfaches Kommunikationsmodell	8
2.1.3	Informationsgehalt und Entropie	9
2.1.4	Gegenseitige Information	13
2.1.5	Die Kanalkapazität	15
2.2	Quanteninformationstheorie	16
2.2.1	Quantales Zweiniveausystem	17
2.2.2	Die von Neumann-Entropie	22
2.2.3	Die Messung	23
2.2.4	Verschränkung	28

2.1 Klassische Informationstheorie

2.1.1 Einführung

Die klassische Informationstheorie beschäftigt sich mit der Kommunikation zwischen zwei oder mehreren Parteien und wurde hauptsächlich durch SHANNON 1948 begründet

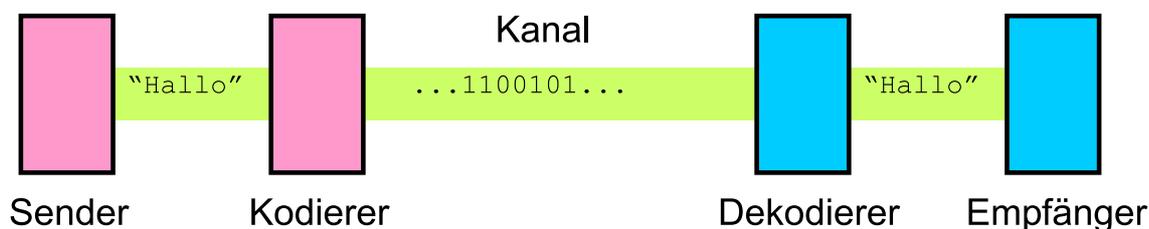


Abbildung 2.1: Der klassische Kanal

[6]. Er untersuchte das Problem, dass eine Nachricht von einer Stelle – dem Sender – über einen so genannten Informationskanal zu einer anderen Stelle – dem Empfänger – übermittelt werden soll. Die Nachricht kann auf ihrem Weg über den Kanal verrauscht, also teilweise abgeändert werden, zum Beispiel durch im realen System stets vorhandene Störeinflüsse.

Die Nachricht enthält eine bestimmte *Menge* an Information, die man als das eigentliche Gut des Transports bezeichnen könnte. Eine der großen Leistungen der Shannonschen Theorie ist ein mathematischer Formalismus, der die Quantifizierung dieser Menge an Information erlaubt. Damit wurde es möglich, so wichtige und zentrale Begriffe, wie den Informationsgehalt einer Nachricht oder die Kapazität eines Kanals, exakt zu definieren. Unter anderem konnte man die minimalen Ressourcen bestimmen, die man für bestimmte Vorgänge wie den Transport oder die Speicherung von Nachrichten, beziehungsweise deren Informationsgehalts, benötigt.

Die Nachricht, sowie das Auftreten ihrer Bestandteile, wird dabei rein statistisch behandelt. Über eine etwaige Bedeutung der Information, also wie sie welche Auswirkungen in einem bestimmten Kontext auf uns und die physikalische Welt haben könnte, wie sie also interpretiert wird, macht die Theorie keine Aussagen [6].

In diesem ersten Abschnitt meiner Arbeit werde ich ein paar grundlegende Begriffe der Informationstheorie einführen. Dabei beschränke ich mich im Wesentlichen auf die Themen, die für das Verständnis der Ausführungen in den darauf folgenden Abschnitten notwendig sein werden. Eine zentrale Rolle spielen hierbei die Begriffe der Entropie, der gegenseitigen Information (Kap. 2.1.3) und der Kanalkapazität (Kap. 2.1.5).

2.1.2 Ein einfaches Kommunikationsmodell

Die Kommunikation zwischen zwei Parteien, dem Sender und dem Empfänger, geschieht in einem sehr einfachen Modell folgendermaßen (Abb. 2.1): Der Sender¹ ("Nachrichtenquelle") will eine Nachricht zum Empfänger² schicken; diese Nachricht liegt in einer konkreten Form (Sprache, Schrift, elektronische Datei, eine Funktion der Zeit, ...) vor, die nicht näher spezifiziert, sondern abstrakt behandelt wird. Diese Nachricht wird auf Senderseite vom "Kodierer" in eine Form gebracht, die zur Übertragung über den Kanal geeignet ist. Der Text eines Zeitungsartikels könnte zum Beispiel in diesem Schritt in eine Folge von wohldefinierten Zeichen im ASCII-Code abgebildet werden, die dann in (Spannungs-) Pulse einer digitalen Logik umgesetzt werden. Der Kanal ist das physikalische Medium, das den Informationstransport ermöglicht. Zum Beispiel kann man sich ein Netzkabel, in dem elektrische Pulse laufen, oder die Funkübertragung über elektromagnetische Wellen vorstellen. Aber auch "menschlichere" Medien wie die Luft, in der sich Schallwellen ausbreiten, können als Kommunikationskanal interpretiert werden.

¹Wird häufig mit "Alice" bezeichnet.

²Wird häufig mit "Bob" bezeichnet.

Auf der Empfängerseite sorgt der "Dekodierer" dafür, dass die Signale des Kodierers für den Empfänger wieder verständlich werden, der sie schlussendlich als "Nachrichtsenke" behält. Es soll uns nicht weiter interessieren, was dann damit geschieht, also ob der Empfänger die Nachricht vielleicht speichert, weiterschickt oder verarbeitet.

Häufig spielt bei allgemeinen Betrachtungen der Nachrichtenübertragung die Unterscheidung zwischen Nachrichtenquelle und Kodierer beziehungsweise zwischen Nachrichtsenke und Dekodierer eine untergeordnete Rolle – im Gegensatz zu dem sehr reichen Feld der *Kodierungstheorie*, die sich unter anderem mit der Frage beschäftigt, wie man möglichst effizient – also unter Verwendung möglichst geringer zeitlicher oder räumlicher Ressourcen – Nachrichten ohne Verlust der Information in eine andere Form überführen (kodieren) kann.

Dieses Modell dient nur dazu, sich eine Vorstellung von dem Prozess der Nachrichtenübertragung zu machen. Wir werden es im Folgenden noch verfeinern und mathematisch beschreiben.

2.1.3 Informationsgehalt und Entropie

Eine *diskrete* Quelle besitzt einen endlichen Vorrat von N Symbolen

$$A = \{a_1, a_2, \dots, a_N\}, \quad (2.1)$$

aus dem zum Zweck der Nachrichtenübertragung eine wiederum diskrete und endliche Sequenz von Symbolen ausgewählt und versendet wird. A heißt Alphabet oder Symbolvorrat der Quelle; seine Elemente werden Zeichen oder Symbole genannt.

Alternativ kann man kontinuierliche Symbolmengen zulassen; wir beschränken uns hier auf den diskreten Fall. Die Quelle heißt *gedächtnislos*, wenn die Auswahl der Symbole statistisch unabhängig erfolgt.

Man kann die Quellennachricht als eine Folge von unabhängigen und identisch verteilten (u.i.v.) Zufallsvariablen X_1, X_2, \dots modellieren, wobei jedes X_i ($i = 1, 2, \dots$) die Werte a_1, a_2, \dots, a_N mit den Wahrscheinlichkeiten $p(a_1), p(a_2), \dots, p(a_N)$ annimmt. Diese Wahrscheinlichkeiten versteht man als relative Häufigkeiten der Symbole a_i in einer großen Menge von Nachrichten, da ihr Vorkommen ja nicht zufällig, sondern vom Sender bestimmt ist. Es gilt $\sum_{i=1}^N p(a_i) = 1$ und $p(a_i) > 0$, da nicht auftauchende Symbole aus A gestrichen werden können.

Betrachtet man etwa einen Text in deutscher Sprache als Nachricht, so haben die X_i Werte, die die Buchstaben des Alphabets darstellen und die $p(a_i)$ geben die relative Häufigkeit der einzelnen Buchstaben in typischen deutschen Texten an, z.B.³ $p(a_1) = p('a')$.

³An diesem Beispiel erkennt man, dass die Unabhängigkeit der X_i in realen Systemen nicht immer gegeben ist, so wird z.B. $X_{i+1} = 'i'$ nach $X_i = 'e'$ mit größerer Wahrscheinlichkeit auftreten, als an einer beliebigen Stelle in der Nachricht.

Informationsgehalt

Wenden wir uns der Frage zu, wie viel Information vom Sender zum Empfänger gelangt, wenn diesen ein bestimmtes Zeichen $X = x \in A$ erreicht. Es ist klar, dass die Menge an Information die den Empfänger beim Auftreten dieses Ereignisses erlangt, nicht vom Symbol selbst abhängt (sei es ein 'a', eine '0' oder ein '♥'), sondern nur durch die Wahrscheinlichkeit $p(x)$ seines Auftretens in allgemeinen Nachrichten bestimmt ist.

Man kann sich zum Beispiel ein Spiel mit einer Münze vorstellen, bei dem in Abhängigkeit vom Auftreten des Symbols "Kopf" oder "Zahl" bestimmte Ereignisse geschehen sollen (wie zum Beispiel bei einer Wette). Dann ist es vollkommen unerheblich, wie die Münze aussieht, sprich welche konkrete "Form" das Symbol hat. Wichtig ist nur die Wahrscheinlichkeit, mit der die Symbole auftreten, hier jeweils 50%.

Ist $p(x) = 1$ (und somit $p(y) = 0$ für alle anderen Zeichen $y \neq x$), so kann das Zeichen x keine Information übertragen, da sein Auftreten sicher (vom Empfänger vorhersagbar) ist. Dementsprechend kann einem sehr "seltenen" Symbol x , also $0 < p(x) \ll 1$, ein hoher Informationsgehalt zugeordnet werden.

Folgende Überlegung macht das plausibel: Stellen wir uns vor, wir würden die Buchstaben einer deutschen Textnachricht binär kodieren, also jedem Buchstaben einen endlichen "Bitstring" – eine Folge von Nullen und Einsen – zuordnen; und zwar möchten wir das möglichst effizient machen, die Länge des Bitstrings also möglichst gering halten. Dann wird man häufig vorkommenden Buchstaben (p groß) wie 'e' oder 'a' eine sehr kurze Sequenz zuordnen, seltenen (p klein) wie 'y' oder 'q' einen längeren. Umgekehrt gesehen erhalten wir nun durch das Auftreten des Buchstabens 'q' viel mehr Information über den Bitstring als von einem 'a'. Man benötigt also mehr Bit, um die Information eines seltenen Buchstabens zu speichern.

Wir fordern daher, dass der noch zu definierende Informationsgehalt $I(x)$ eines Symbols x umso höher sei, je unwahrscheinlicher bzw. seltener sein Auftreten ist. Ferner soll sich die gesamte übertragene Information einer Nachricht der Länge L aus der Summe der Informationsgehalte seiner Zeichen zusammensetzen

$$I(\text{Nachricht}) = I(x_1) + I(x_2) + \dots + I(x_L).$$

Unter diesen Bedingungen kommt man auf sehr natürliche Weise [6] auf das logarithmische Informationsmaß

$$I(x) := -\log_2 p(x) \geq 0, \quad x \in A \tag{2.2}$$

Die Basis des Logarithmus ist grundsätzlich frei wählbar. Eine Definition in einer anderen Basis $b > 0$ impliziert lediglich einen konstanten Faktor $\log_2 b$ im Informationsgehalt. Wir folgen der weithin üblichen Konvention, den Logarithmus zur Basis zwei zu nehmen und die Einheit ein "bit" (engl. *basic indissoluble information unit* – nicht weiter auflösbare Informationseinheit) zu nennen⁴.

⁴Wir unterscheiden zwischen der informationstheoretischen Einheit "bit" und der zweiwertigen Größe

Das Anhängen des Wortes "bit" an den strenggenommen dimensionslosen Wert des Informationsgehaltes erinnert also explizit an unsere Wahl der Basis 2.

Beispiel

Hat man ein zweiwertiges Alphabet $A = \{a_1 = 0, a_2 = 1\}$ vorliegen, deren zwei Zeichen mit gleicher Wahrscheinlichkeit $p = p(a_1) = p(a_2) = \frac{1}{2}$ auftreten, so kann auch jedes übertragene und vom Empfänger ausgelesene $X = x \in A$ die zwei Werte 0 oder 1 annehmen und somit genau 1 bit Information übertragen:

$$I_x = -\log \frac{1}{2} = 1 \text{ bit.}$$

Ein Bitstring der Länge n , also n solcher Zeichen zusammen, hat einen Wertebereich von 2^n Zuständen aus $\{0, 1\}^n$ und kann bei Gleichverteilung ($p = \frac{1}{2^n}$) dementsprechend

$$I_n = -\log \frac{1}{2^n} = n \text{ bit}$$

repräsentieren. An dieser Stelle wird die logarithmische Definition des Informationsgehaltes plausibel, da n Zeichen, von denen jedes 1 bit Information trägt, $n \cdot 1 \text{ bit} = n \text{ bit}$ kodieren können, während ihr Wertevorrat exponentiell mit der Länge der Zeichenkette wächst.

Entropie

Eine zentrale Rolle in der Informationstheorie nimmt die (Shannon-) Entropie $H(X)$ einer Zufallsvariable ein. Die Bezeichnung *Entropie* verdankt diese Größe ihrer - nicht nur formalen - Ähnlichkeit mit der gleichnamigen Größe aus der statistischen Thermodynamik, die die Unordnung eines Systems beschreibt. Es ist in diesem Umfeld sehr hilfreich, mit der Entropie zwei Vorstellungen zu verknüpfen und sich klar zu machen, dass sie äquivalent sind: Die Entropie einer Zufallsvariable⁵ X ist ein Maß für

1. die *Unsicherheit* über den tatsächlichen Wert von X *bevor* man ihn erfährt.
2. die *Information*, die man gewonnen hat, *nachdem* man Kenntnis vom tatsächlichen Wert von X erlangt hat.

Wir definieren die Entropie formal als den mittleren Informationsgehalt der Zufallsvariable X :

$$H(X) := \sum_x p(x) \cdot I(x) = - \sum_x p(x) \cdot \log p(x). \quad (2.3)$$

⁵"Bit" (engl. *binary digit*), die nur 0 oder 1 sein kann und genau 1 bit Information repräsentieren kann. Schreibe die Basis im Folgenden nicht mehr mit an: $\log := \log_2$.

⁵Da die Entropie nur von der Wahrscheinlichkeitsverteilung $p_X \equiv \{p(x)\}_x \in A$ abhängt, ist es bei u.i.v. Variablen äquivalent, von der Entropie der Zufallsvariable, der Quelle oder einer Nachricht zu sprechen.

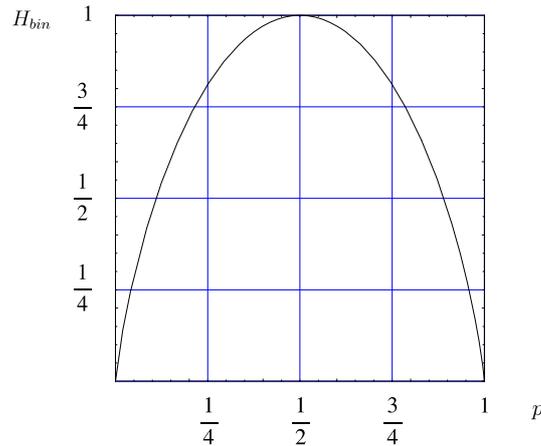


Abbildung 2.2: Die binäre Entropie als Funktion der Wahrscheinlichkeit $p = p(0) = 1 - p(1)$. Man beachte die Symmetrie $H_{bin}(p) = H_{bin}(1 - p)$.

Sie hängt nur von der Wahrscheinlichkeitsverteilung $p \equiv p_X$ von X ab und ist somit mathematisch exakter formuliert ein Funktional auf der Menge der Wahrscheinlichkeitsverteilungen⁶. Ab hier können wir auch $p(x) = 0$ zulassen, wenn wir $0 \log 0 := 0$ definieren, was durch eine Grenzwertbetrachtung leicht gerechtfertigt werden kann.

Eine wichtige Interpretation der Entropie folgt aus Shannons Theorem zum rauschfreien Kodieren [6, 7], das besagt, dass man im Mittel $H(X)$ bit pro Quellenzeichen benötigt, um die gesamte Information der Nachricht zu kodieren (oder zu speichern), wenn $H(X) = H(X_1) = H(X_2) = \dots$ die Entropie der Quelle ist. Eine verlustfreie Kompression unter diese Marke ist nicht möglich, d.h. $H(X)$ ist ein sehr vernünftiges Maß für die Information einer Nachricht – die ja unabhängig vom Kompressionsgrad sein soll. Aus der Definition folgt, dass sie genau bei Gleichverteilung ($\forall x \in A : p(x) = \frac{1}{N}$, wo $N := |A|$) maximal und gleich dem konstanten, für alle x gleichen, Informationsgehalt $I(x) = \log N$ ist:

$$H(X) \leq \log |A| \quad \text{und} \quad H(X) = \log |A| \Leftrightarrow X \text{ gleichverteilt} \quad (2.4)$$

Beispiel: Binäre Entropie

Eine Nachricht aus einer zweiwertigen und u.i.v. Quelle mit

$$A = \{0, 1\}, \quad p(0) = p, \quad p(1) = 1 - p \quad (2.5)$$

⁶Ich verzichte auf den Index X in $p_X(x)$, wenn klar ist, dass die Verteilung der Variable X gemeint ist. Man beachte, dass somit $p(x) \neq p(y)$ auch für $x = y$ sein kann, da zwei verschiedene Verteilungen p_X bzw. p_Y gemeint sind.

bei der an jeder Stelle mit Wahrscheinlichkeit $0 \leq p \leq 1$ eine 0 bzw. $1 - p$ eine 1 steht, hat die Entropie

$$H(X) = H_{bin}(p) := -(p \cdot \log p + (1 - p) \cdot \log(1 - p)) \quad (2.6)$$

pro Zeichen (siehe Abb. 2.2). Die Entropie ist maximal, nämlich $H(X) = 1$ bit für eine gleichverteilte Quelle, $p = 1 - p = \frac{1}{2}$. $H(X) = 0$, wenn $p = 1$ ($p = 0$), da die Nachricht dann nur mehr aus Nullen (Einsen) besteht und keine Information mehr trägt.

Ein fairer Münzwurf [7] ($p = \frac{1}{2}$) hat demnach $H = 1$ bit.

2.1.4 Gegenseitige Information

Quell- und Zielsymbolvorrat A_X und A_Y müssen nicht notwendigerweise übereinstimmen. Im allgemeinsten Fall kommt von der Quelle eine per p_X verteilte Größe X über den Kanal, die gemäß einer bedingten Wahrscheinlichkeitsverteilung $p(y|x)$ das Ereignis $Y = y$ beim Empfänger auslöst. Die Verteilung von Y ist dann vorgegeben; ich nenne sie p_Y .

$p(y|x)$ ist die (bedingte) Wahrscheinlichkeit, dass der Empfänger $Y = y$ sieht, unter der Voraussetzung, dass der Sender $X = x$ schickte. Die $|A_Y| \times |A_X|$ -Matrix mit den Einträgen $p(y|x)$ ($x \in A_X, y \in A_Y$) wird daher auch Transfermatrix genannt.

Was lernt der Empfänger aus dem Auftreten des Symbols $Y = y$ über das gesendete Symbol $X = x$? Oder mit anderen Worten: wie viel Information über das gesendete Symbol enthält das empfangene Symbol? Die Antwort gibt die gegenseitige Information $I(X : Y)$,

$$I(X : Y) := \sum_{x,y} p(x,y) \cdot \log \frac{p(x,y)}{p(x) \cdot p(y)} \quad (2.7)$$

Die $p(x,y)$ sind die gemeinsamen Wahrscheinlichkeiten, dass x gesendet *und* y empfangen wird. Die Bezeichnung "gegenseitig" rührt von der Symmetrie $I(X : Y) = I(Y : X)$ her, die man direkt aus der Definition ablesen kann.

Man kann die gegenseitige Information von X und Y verstehen als die über alle $x \in A_X$ und $y \in A_Y$ gemittelte Distanz⁷ zwischen der gemeinsamen Verteilung $p(x,y)$ und dem Produkt ihrer Einzelverteilungen $p(x) \cdot p(y)$.

Die gegenseitige Information ist null, d.h. aus Y kann überhaupt nicht auf X geschlossen werden, wenn X und Y statistisch unabhängig sind, also $p_{XY} = p_X \cdot p_Y$. In diesem Fall wird keine Information übertragen, da gesendete und empfangene Daten gänzlich *unkorreliert* sind. Eine kurze Rechnung ergibt ferner

$$I(X : Y) \leq H(X), \quad I(X : Y) \leq H(Y). \quad (2.8)$$

Dieses interessante Resultat werden wir im nächsten Abschnitt über die Kanalkapazität interpretieren.

⁷Gemeint ist die Kullback Leibler Distanz bzw. die relative Entropie der Verteilungen [8].

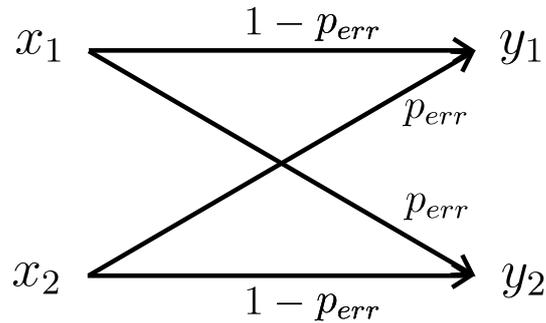


Abbildung 2.3: Ein symmetrischer binärer Kanal mit Fehlerwahrscheinlichkeit p_{err} .

Beispiel: Symmetrischer binärer Kanal

In einer Situation, wie sie in Abb. 2.3 schematisiert ist, sind auf Sender- und Empfängerseite je zwei verschiedene Symbole erlaubt, also $A_X = \{x_1, x_2\}$, $A_Y = \{y_1, y_2\}$. Dabei tritt bei der Übertragung jedes Zeichens mit Wahrscheinlichkeit p_{err} ein "Fehler" auf, was bedeuten soll, dass durch den Kanal $x_1 \mapsto y_2$ oder $x_2 \mapsto y_1$ abgebildet wird.

Für einen rauschfreien Kanal gilt $p_{err} = 0$. Ist die Entropie der Quelle maximal, also $H(X) = 1$ bit, impliziert dies $p(x_1) = p(x_2) = \frac{1}{2}$ und damit $I(X : Y) = 1$ bit⁸. Die Transfermatrix ist im Fall $p_{err} = 0$ die Einheitsmatrix. Der Empfänger in diesem Fall also die volle Information über die Nachricht erhalten, während Rauschen auf dem Kanal ($0 < p_{err} < 1$) die gegenseitige Information reduziert:

Im Allgemeinen Fall man die Elemente der Transfermatrix des symmetrischen binären Kanals als

$$p(y_1|x_1) = 1 - p_{err} \quad p(y_1|x_2) = p_{err} \quad (2.9)$$

$$p(y_2|x_1) = p_{err} \quad p(y_2|x_2) = 1 - p_{err} \quad (2.10)$$

mit $0 \leq p_{err} \leq 1$ schreiben.

Tritt bei der Übertragung ein Fehler, also $x_i \rightarrow y_j$, $i \neq j$ mit Wahrscheinlichkeit p_{err} auf, so gilt [8]

$$I(X : Y) \leq 1 - H_{bin}(p_{err}). \quad (2.11)$$

Wenn $p_{err} = \frac{1}{2}$, ist $H_{bin}(p_{err}) = 1$ bit und damit $I(X : Y) = 0$, schließlich ist das Auftreten von $Y = y_{1/2}$ in diesem Fall vollkommen zufällig und unabhängig von X . Man beachte, dass $I(X : Y)$ wieder maximal für $p_{err} = 1$ ist. Dann werden nämlich alle Symbole deterministisch vertauscht, was äquivalent zum rauschfreien Kanal nach Neudefinition des Alphabets zu $A'_Y := \{y'_1 = y_2, y'_2 = y_1\}$ ist (vgl. dazu Abb. 2.2)!

⁸Da die Zeichen bijektiv aufeinander abgebildet werden, gilt dann natürlich $H(Y) = H(X)$.

Für $p_{err} = 0$ ergibt sich in Übereinstimmung mit dem oben gesagten $H_{bin}(p_{err}) = 0$, und damit $I(X : Y) = 1$ bit.

2.1.5 Die Kanalkapazität

Wenden wir uns nun Frage zu, wieviel Information vom Sender zum Empfänger über einen bestimmten Kanal maximal gelangen kann, der sogenannten Kanalkapazität. Bei gegebener Sendefrequenz definiert diese Größe die maximale Transmissionsrate. Denkt man etwa an die Verbindung zweier Rechner über ein Netzwerk, so ist es wichtig zu wissen, wie viel Information vom einen zum anderen über das Netzwerkkabel während einer bestimmten Zeitspanne übertragen werden kann.

Im vorigen Abschnitt haben wir gesehen, dass die Information, die Sender und Empfänger über einen Kanal austauschen können, durch den Ausdruck (2.7) gegeben ist. Schreibt man diesen zunächst ein wenig um, indem man $p(x, y) = p(y|x)p(x)$ sowie $p(y) = \sum_x p(y|x)p(x)$ in Gl. 2.7 einsetzt, so erhält man

$$I(X : Y) = \sum_{x,y} p(y|x) p(x) \cdot \log \frac{p(y|x)}{\sum_{x'} p(y|x') p(x')}. \quad (2.12)$$

Daraus können wir ablesen, dass $I(X : Y)$ nur von der Transfermatrix $p(y|x)$ des Kanals sowie der Wahrscheinlichkeitsverteilung p_X und damit der Entropie $H(X)$ der Quelle abhängt. Da wir die Kapazität des Kanals selbst – also die maximale Menge von Information unabhängig von der Quelle oder ihrer Nachrichten bzw. deren Verteilungen – definieren wollen, schreiben wir

$$C := \max_{\{p_X\}} I(X : Y). \quad (2.13)$$

Das Maximum ist über alle Verteilungen der Quelle zu bilden. C ist somit unabhängig von der Verteilung der Quelle und ausschließlich gegeben durch seine Transfermatrix. Eine verlustfreie Übertragung von Information jenseits der Kanalkapazität ist nicht möglich.

In Abb. 2.4 ist die Kapazität des symmetrischen binären Kanals (siehe oben), $C = 1 - H_{bin}(p_{err})$ gezeigt. Sie ist maximal, wenn kein Rauschen auftritt, und $C = 0$, wenn der Kanal vollkommen verrauscht ist.

Wegen Gl. 2.8, 2.4 ist

$$C \leq \min\{H(X), H(Y)\} \leq \min\{\log |A_X|, \log |A_Y|\}. \quad (2.14)$$

Die Kapazität eines Kanals zwischen einer Quelle mit $|A_X|$ Zeichen und einem Empfänger mit einem Alphabet von $|A_Y|$ Zeichen kann also nicht größer werden als der Logarithmus der Mächtigkeit des kleineren Alphabets. Insbesondere kann Bob nie mehr Information einfach dadurch erhalten, dass er sein Alphabet einseitig vergrößert (größer als das von Alice).

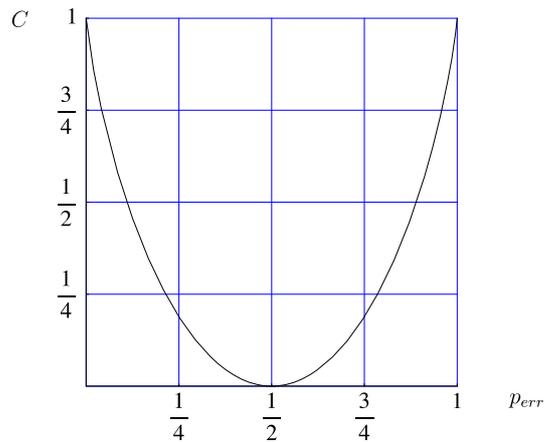


Abbildung 2.4: Die Kapazität C des symmetrischen binären Kanals in Abhängigkeit der Fehlerwahrscheinlichkeit p_{err} .

Beispiel

Ist das Alphabet auf Sender- und Empfängerseite zweiwertig $|A_X| = |A_Y| = 2$, folgt gemäß Gl. 2.14 und 2.4, dass $C \leq \log 2 = 1$ bit ist. Diese obere Grenze wird auch tatsächlich erreicht, wenn die Quelle gleichverteilt und der Kanal rauschfrei ist, wie wir weiter oben in diesem Abschnitt gesehen haben. Andererseits kann die Kapazität des Kanals auch null sein (vgl. Gl. 2.11), wenn das Rauschen maximal und statistisch ist.

Bei vierwertigen Alphabeten $|A_X| = |A_Y| = 4$, also zum Beispiel

$A_X = A_Y = \{00, 01, 10, 11\}$, kann die Kapazität nie größer als $H(X) = H(Y) = \log 4 = 2$ bit sein. Eine *einseitige* Vergrößerung des Alphabets – etwa in dem Fall, dass der anderen Partei diese Maßnahme nicht mitgeteilt werden kann – kann keine Erweiterung der Kanalkapazität über 2 bit, und damit auch keinen Informationsaustausch mit mehr als 2 bit pro Symbol, bewirken.

2.2 Quanteninformatiionstheorie

Im vorigen Abschnitt befassten wir uns mit der Frage, wie man Information mathematisch beschreiben kann. Es ist wichtig sich klarzumachen, dass jedem Vorgang, bei dem Information transportiert, verarbeitet oder gespeichert wird, ein physikalischer Prozess zugrunde liegt. Man denke zum Beispiel an die menschliche Sprache, die Informationsübertragung in oder zwischen elektronischen Rechnern, oder die Signalverarbeitung im Gehirn. Stets ist ein physikalisches Medium (Schallmedium, elektrische Leitungen, elektromagnetische Wellen, synaptische Verbindungen etc.) vorhanden, das durch seinen Zustand die Information repräsentiert. Übergänge zwischen verschiedenen Zuständen können als Verarbeitung der Information gedeutet werden.

Das informationstheoretisch einfachste nichttriviale System hat genau zwei unterscheidbare Zustände (etwa 0 und 1) und kann somit genau 1 bit Information repräsentieren. Ein solches klassisches Zweiniveausystem wird in jedem elektronischen Rechner millionenfach implementiert. Die zwei Zustände der physikalischen Realisierung werden gemäß der (zweiwertigen) Booleschen Logik interpretiert und verarbeitet.

Ein solches System, das genau ein "Bit" darstellt, wird durch eine sehr großen Anzahl mikroskopischer Teilchen, wie Elektronen, Atome oder Moleküle realisiert. Untersucht man jedoch die Situation, dass die Information in den Zuständen einzelner Teilchen kodiert wird, ergeben sich vollkommen neue Möglichkeiten.

Die Objekte, mit denen wir es nämlich dann zu tun haben, folgen nicht mehr den Gesetzen der klassischen Physik, sondern müssen durch die Quantentheorie beschrieben werden; und deren Implikationen haben uns schon mehr als einmal dazu gezwungen, unsere Vorstellungen von der Welt des Allerkleinsten zu revidieren oder zumindest zu erweitern.

2.2.1 Quantales Zweiniveausystem

Definition des Qubits

Das quantale Zweiniveausystem wird in Analogie zum klassischen Fall "Qubit" genannt und den Prinzipien der Quantenmechanik gemäß durch einen Vektor $|\psi\rangle$ in einem zweidimensionalen komplexen Hilbertraum \mathbb{H}_2 beschrieben. Dessen – grundätzlich beliebig ausgezeichnete – Basisvektoren nennen wir $|0\rangle \doteq \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $|1\rangle \doteq \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, also $\mathbb{H}_2 = \text{span}\{|0\rangle, |1\rangle\}$ (der Punkt auf dem Gleichheitszeichen soll daran erinnern, dass das Gebilde rechts davon nur die Darstellung in einer bestimmten Basis ist).

Im entscheidenden Gegensatz zum klassischen Fall ist der (reine) Zustand $|\psi\rangle$ des Qubit wegen der Möglichkeit kohärenter Superposition der Basiszustände

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \doteq \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C} \quad (2.15)$$

nicht mehr durch einen einzigen binären Wert vollständig charakterisierbar, sondern durch zwei komplexe Größen α und β . Die Normierung des Zustandes ergibt die Forderung

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2.16)$$

Mit den Definitionen

$$e^{i\varphi} \cos \frac{\theta}{2} := \alpha, \quad e^{i(\varphi+\phi)} \sin \frac{\theta}{2} := \beta, \quad \theta \in [0, \pi], \quad \varphi \in [0, 2\pi[, \quad \phi \in [0, 2\pi]. \quad (2.17)$$

schreibt sich Gl. 2.15 dann als $|\psi\rangle = e^{i\varphi} (\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle)$. Der globale Phasenfaktor $e^{i\varphi}$ beeinflusst nicht das Ergebnis einer Messung an diesem Zustand [7], er kann also

weggelassen werden. Unser Qubit ist damit charakterisiert durch zwei reelle Parameter θ und ϕ :

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \quad \theta \in [0, \pi], \quad \phi \in [0, 2\pi[\quad (2.18)$$

Die Blochsphäre

Der komplexe zweidimensionale Vektor $|\psi\rangle$ des reinen Qubit Zustands kann entsprechend 2.18 durch einen Punkt auf der Oberfläche der dreidimensionalen Einheitskugel – die in diesem Zusammenhang *Blochsphäre* genannt wird – mit den Kugelkoordinaten $(r = 1, \theta, \phi)$ visualisiert werden (Fig. 2.5).

Der Vektor vom Ursprung zu $(r = 1, \theta, \phi)$ heißt "Blochvektor". Orthogonale Zustände $|\psi_1\rangle$ und $|\psi_2\rangle$, also Zustände, für die $\langle\psi_1|\psi_2\rangle = 0$ gilt, entsprechen gegenüberliegenden Punkten auf der Blochsphäre.

Die Zustände

$$\begin{aligned} |P\rangle &:= \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \\ |M\rangle &:= \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \\ |L\rangle &:= \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle) \\ |R\rangle &:= \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle) \end{aligned} \quad (2.19)$$

definieren die zu $\{|0\rangle, |1\rangle\}$ konjugierten⁹ Basen $\{|P\rangle, |M\rangle\}$ bzw. $\{|L\rangle, |R\rangle\}$.

Die Notation antizipiert die Interpretation als unter **plus/minus** 45° linear bzw. **rechts-/linkszirkular** polarisierten Photonen.

Besonders den beiden ersten Zuständen aus Gl. 2.19 werden wir in dieser Arbeit noch sehr häufig begegnen.

Bei "fahrlässig klassischer" Betrachtung scheint es möglich, in einem einzigen Qubit-Zustand – der ja nach Kap. 2.2.1 durch zwei reelle Parameter θ, ϕ charakterisiert ist – nahezu beliebig viel Information zu speichern und mit ihm zu transportieren. Immerhin besteht die Blochsphäre aus unendlich vielen Punkten!

Zum Beispiel könnte man den Inhalt seiner Festplatte als Binärdarstellung einer oder zweier reeller Zahlen interpretieren, auf geeignete Bereiche skalieren und in θ und/oder ϕ kodieren, was zwar experimentelle, nicht jedoch prinzipielle Probleme birgt.

Dieses System könnte nun zu einer anderen, entfernten Partei gesendet und von dieser ausgelesen werden, sodass mit denkbar geringen Ressourcen (einem einzigen Quant) eine beliebig große Menge Information übermittelt worden wäre.

⁹Alle Basiszustände *einer* Basis sind in einer *anderen* Basis vollkommen ununterscheidbar; in \mathbb{H}_2 gibt es jeweils Tripel von paarweise konjugierten Basen.

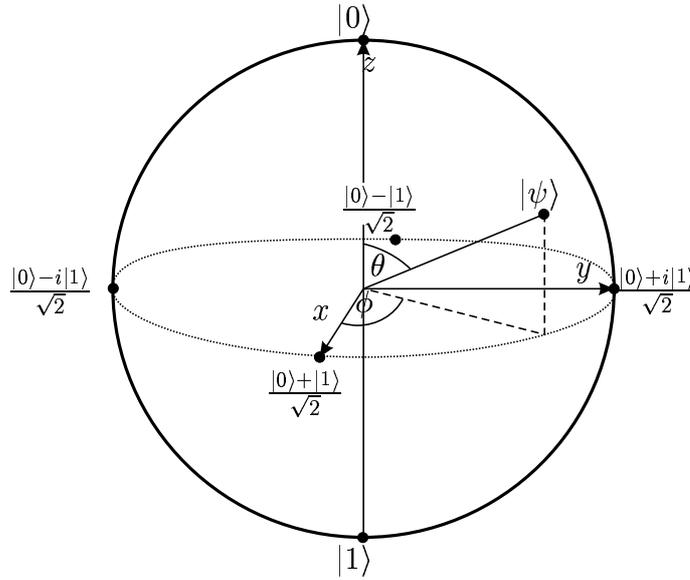


Abbildung 2.5: Jeder Qubit-Zustand $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ kann auf der Blochsphäre dargestellt werden.

Wie ich später noch genauer darlegen werde, ist dies nicht möglich. Das liegt daran, dass das Ergebnis einer Messung an einem einzigen Exemplar eines Qubit-Zustandes (also zum Beispiel einem einzigen Photon) keinen vollständigen Rückschluss auf den Zustand, der dieses Resultat bedingt haben könnte, zulässt. Es gibt immer unendlich viele andere Zustände, die das gleiche Resultat mit endlicher Wahrscheinlichkeit liefern.

Operationen auf dem Qubit

In der Quantentheorie ist nicht nur der (Hilbert-) Raum der Zustände linear, sondern auch alle Operationen O auf diesen Zuständen: Ist $\{|\psi_i\rangle\}_{i=1}^N$ eine beliebige Menge von Vektoren aus dem Hilbertraum und $|\psi\rangle = \sum_i c_i |\psi_i\rangle$, $c_i \in \mathbb{C}$, so gilt

$$O|\psi\rangle = O\left(\sum_i c_i |\psi_i\rangle\right) = \sum_i c_i (O|\psi_i\rangle) \quad (2.20)$$

Deswegen hat jeder Operator O , der auf Zuständen aus unserem Qubit-Raum \mathbb{H}_2 operiert, eine eindeutige Repräsentation als 2×2 -Matrix, wenn vorher definiert worden ist, in welcher Basis die Darstellung erfolgt. Wenn nichts anderes gesagt wird, verwenden wir immer die Standardbasis $\{|0\rangle, |1\rangle\}$.

Unitäre Operatoren

In der Quanteninformationstheorie sind unitäre Operatoren U , $U^{-1} = U^\dagger$ von besonderer Bedeutung. Sie beschreiben eine Evolution des quantalen Systems, in der kein Teilchenverlust auftritt. Insbesondere ist die unitäre Evolution reversibel. Es tritt keine Dekohärenz auf, die durch Wechselwirkung mit der Umwelt geschehen kann.

In der Matrixdarstellung eines unitären Operators müssen sowohl seine Zeilen-, als auch seine Spaltenvektoren normiert und orthogonal sein.

Das Skalarprodukt ist invariant unter unitären Operatoren,

$$\langle U\psi_1 | U\psi_2 \rangle = \langle \psi_1 | U^\dagger U | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle \quad (2.21)$$

und insbesondere bleiben orthogonale Zustände nach der Transformation orthogonal – also in der mitgedrehten Basis gänzlich unterscheidbar. Unter realen experimentellen Bedingungen hat man allerdings stets mit der Nichtunitarität (Absorption, thermische Einflüsse etc.) der Systementwicklung zu rechnen. Ein großer Vorteil von quantalen photonischen Systemen ist die geringe Dekohärenz, also die geringe unerwünschte Beeinflussung durch die Umwelt.

Spezielle unitäre Operatoren

Die Vektoren der Standardbasis und der zu ihr konjugierten Basen (vgl. Gl. 2.19) sind Eigenvektoren der durch die Pauli-Matrizen dargestellten unitären und hermiteschen Operatoren

$$\begin{aligned} \sigma_x &= |P\rangle\langle P| - |M\rangle\langle M| && \doteq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= |L\rangle\langle L| - |R\rangle\langle R| && \doteq \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= |H\rangle\langle H| - |V\rangle\langle V| && \doteq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \quad (2.22)$$

mit den Eigenwerten ± 1 . Zusammen mit der Identität $\mathbb{1}$ bilden diese drei Operatoren einen vollständigen Satz, d.h. jeder Operator A auf \mathbb{H}_2 kann als komplexe Linearkombination $A = c_0\mathbb{1} + c_1\sigma_x + c_2\sigma_y + c_3\sigma_z$, $c_0, \dots, c_3 \in \mathbb{C}$ geschrieben werden.

Auf dieser Tatsache basiert zum Beispiel die so genannte Zustandsstomographie, die eine vollständige Charakterisierung des (nicht notwendig reinen) Qubitzustandes erlaubt, wobei die Mittelwerte der Operatoren aus Gl. 2.22 durch wiederholte Messung an vielen gleichen Exemplaren des Zustands ermittelt werden.

Im Speziellen kann jeder positive Operator mit Spur gleich 1, also jeder Dichteoperator mit einem geeigneten Vektor $\vec{r} \in \mathbb{R}^3$ durch

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{r} \cdot \vec{\sigma}), \quad \text{wo } \vec{\sigma} := \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix} \quad (2.23)$$

ausgedrückt werden. Der Vektor \vec{r} repräsentiert ρ in der Blochsphäre. In der Tat stellt diese Definition eine Verallgemeinerung des Falles reiner Zustände dar. Es gilt $\|\vec{r}\| \leq 1$ und Gleichheit (Oberfläche der Kugel!) genau für reine Zustände.

Der Dichteoperator beschreibt neben den reinen Zuständen so genannte gemischte Zustände, die als statistisches Gemisch von Zuständen verstanden werden können. Durch Messung kann man über einen gemischten Zustand nie vollständige Information erlangen, da die Projektion seines Blochvektors auf alle Achsen immer kleiner als eins ist, d.h. es gibt keine Basis, in der die Messung voraussagbar wäre.

Photonische Qubits

In unserem Experiment realisieren wir die Qubits durch die Polarisationszustände einzelner Photonen und -paare. Der Vorteil in der Polarisationskodierung liegt zum einen an der geringen Dekohärenz, also unkontrollierten Wechselwirkung mit der Umwelt der Lichtquanten, und zum anderen daran, dass sie einen Transport über makroskopische Distanzen ermöglichen, im Gegensatz zu Implementierungen durch einzelne Atome oder Ionen.

Unter realen Bedingungen, also außerhalb des Labors, konnte somit Information mit photonischen Qubits über mehr als 20 km in Luft ausgetauscht werden [9]. In Fasern tritt das Problem der Doppelbrechung auf, die jedoch kompensiert werden kann (siehe Kap. 4.5.1).

Außerdem lassen sich unitäre Qubit-Operationen am einzelnen Teilchen sehr leicht durch Wellenplättchen realisieren, die einen Phasenschub zwischen zwei Polarisationsrichtungen bewirken. In der Tat kann man leicht zeigen, dass eine Kombination von Viertel-Halb- und Viertelwellenplättchen nacheinander genügt, um *alle* unitären Transformationen auf \mathbb{H}_2 durchzuführen.

Unsere Standardbasis-Vektoren nennen wir $|H\rangle \equiv |0\rangle$ für horizontale bzw. $|V\rangle \equiv |1\rangle$ für vertikale Polarisationsrichtung. Wie schon erwähnt, benutzen wir die Symbole $|P\rangle, |M\rangle, |L\rangle, |R\rangle$ für Polarisationszustände unter $\pm 45^\circ$ sowie links-/rechtszirkulares Licht. Hier tritt eine Besonderheit der masselosen Photonen in Erscheinung, die bewirkt, dass man, um z.B. den Zustand $|P\rangle$ zu präparieren einen Polarisator um 45° gegen die $|H\rangle$ entsprechende Horizontale drehen muss, wogegen in massiven Systemem (Atomen,...) dieser Zustand einer zu $|0\rangle$ senkrechten Raumrichtung entspricht¹⁰.

¹⁰Da das Photon ein Spin-1 Teilchen ist, entspricht der Drehung der linearen Polarisation im (physika-

2.2.2 Die von Neumann-Entropie

In Kap. 2.1.3 haben wir gesehen, dass die (Shannon-) Entropie $H(X)$ so interpretiert werden kann, dass sie den Informationsgewinn darstellt, wenn man Kenntnis über den tatsächlichen Wert der zufällig verteilten Größe X erhält.

Wegen der intrinsischen Probabilistik Quantenmechanik können wir im Allgemeinen jedoch nicht mehr von "dem Wert" eines quantalen Systems bzw. einem eindeutigen Messwert am Zustand sprechen. Wie wir in Kap. 2.2.3 ausführlich darlegen werden, ist im Allgemeinen nicht die gesamte Information über den Zustand zugänglich.

Die quantenmechanische Nachrichtenübertragung kann man sich in Analogie zum klassischen Fall so vorstellen, dass Alice mit Wahrscheinlichkeit $0 \leq p_i \leq 1$ den Zustand $|\psi_i\rangle$ für $i = 1, \dots, N$ präpariert ($\sum_i p_i = 1$).

Ein Zeichen X befindet sich in dieser Analogie in einem gemischten Zustand ρ ,

$$\rho = \sum_{i=1}^N p_i |\psi_i\rangle \langle \psi_i|. \quad (2.24)$$

Dieser Zustand wird von einem physikalischen, quantalen System zu Bob transportiert ("Quantenkanal"). Bob kann dann eine Messung an ihm durchführen.

Definition

Die (quantale) von Neumann-Entropie eines gemischten Zustands ρ ist

$$S(\rho) := -\text{tr}\{\rho \log \rho\} = -\sum_{i=1}^N \lambda_i \log \lambda_i, \quad (2.25)$$

wo $\lambda_i \geq 0$ ($i = 1, \dots, N := \dim \mathbb{H}$) die Eigenwerte der Dichtematrix ρ sind¹¹. Die rechte Seite von Gl. 2.25 hat die gleiche Form wie die Shannonsche Entropie H (Gl. 2.3) von einer Wahrscheinlichkeitsverteilung¹² $\{p(x_i) = \lambda_i\}_{i=1}^N$. Das wird plausibel, wenn man bedenkt, dass jeder Dichteoperator, also auch ρ , ein hermitescher Operator und damit diagonalisierbar ist. In seiner Spektraldarstellung ist

$$\rho = \sum_i p'_i |\psi'_i\rangle \langle \psi'_i|, \quad (2.26)$$

wobei $p'_i = \lambda_i$ die Eigenwerte der Dichtematrix und $\langle \psi'_i | \psi'_j \rangle = \delta_{ij}$ sind. Man kann den Dichteoperator also so schreiben (Gl. 2.26), dass er aussieht wie ein statistisches En-

lischen) Raum um 45° auch eine Drehung $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ des Zustandsvektors um $\theta = 45^\circ$ – im

Gegensatz zu atomaren Spins, wo konjugierte Basisrichtungen im Raum orthogonal stehen.

¹¹Wie bisher sei der Logarithmus \log zur Basis zwei und $0 \log 0 := 0$ definiert.

¹²Da ρ positiver Dichteoperator ist, sind alle Eigenwerte $\lambda_i \geq 0$ und $\text{tr} \rho = \sum_i \lambda_i = 1$.

semble *orthogonaler* Zustände $\{|\psi'_i\rangle\}_{i=1}^N$ mit der Verteilung¹³ $\{\lambda_i\}_{i=1}^N$. Die orthogonalen Zustände verhalten sich bezüglich ihrer (vollkommenen) Unterscheidbarkeit aber wie klassische Zustände, was dazu führt, dass die klassische Entropie H der Verteilung $\{\lambda_i\}_{i=1}^N$ gleich der von Neumann-Entropie $S(\rho)$ ist.

Aus Gl. 2.25 folgt in Analogie zu Gl. 2.4

$$0 \leq S(\rho) \leq \log N \quad \text{mit} \quad S = 0 \quad \Leftrightarrow \rho = |\psi\rangle\langle\psi| \quad (\text{rein}) \quad (2.27)$$

$$\text{und} \quad S = \log N \quad \Leftrightarrow \rho = \mathbb{1}/N \quad (\text{max. gemischt}). \quad (2.28)$$

Beispiel

Folgendes einfache Beispiel kann den Unterschied zwischen klassischer und von Neumann-Entropie besonders deutlich aufzeigen: Angenommen, Alice generiert mit jeweils 50% Wahrscheinlichkeit einen der Zustände $|H\rangle$ und $|P\rangle$:

$$\rho = \frac{1}{2} (|H\rangle\langle H| + |P\rangle\langle P|) \doteq \frac{1}{4} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \quad (2.29)$$

Bob bekommt diesen Zustand und misst. "Klassisch" betrachtet könnte man meinen, dass Bob die – nicht identischen – Zustände unterscheiden und $H = \log 2 = 1$ bit Information pro Symbol gewinnen könnte, wenn wir einen rauschfreien Kanal betrachten. Dementsprechend würde man mindestens 1 Bit pro Symbol benötigen, um eine Nachricht zu kodieren.

Die Zustände sind allerdings eben nicht klassisch, nicht perfekt unterscheidbar, da $\langle H|P\rangle \neq 0$ ist; ρ hat die zwei Eigenwerte $\lambda_{1/2} = \frac{1}{2}(1 \pm \frac{1}{\sqrt{2}})$. Damit ergibt sich

$$S(\rho) = -(\lambda_1 \log \lambda_1 + \lambda_2 \log \lambda_2) \approx 0.60, \quad (2.30)$$

was nach SCHUMACHERS Theorem, einem quantenmechanischen Pendant zu Shannons rauschfreiem Kodierungstheorem [10, 6], bedeutet, dass $S(\rho) \approx 0.60$ Qubits ausreichen würden, um die Quelle zu kodieren. Wie wir später (Kap. 2.2.3) sehen werden, können durch die zwei quantalen Symbole $|H\rangle$ und $|P\rangle$ nicht mehr als $S(\rho) \approx 0.60$ bit Information übertragen werden.

2.2.3 Die Messung

Der Messvorgang in der Quantenmechanik unterscheidet sich wesentlich von einer Messung im klassischen Sinne. Zwei Eigenschaften zeigen den fundamentalen Gegensatz zur klassischen Situation auf:

Erstens können wir durch eine Messung nicht vollständige Information über den Zustand des quantalen Systems erhalten, wenn wir nur ein Exemplar des Zustands haben. Das

¹³Man kann deswegen überhaupt nicht davon sprechen, dass ρ ein Ensemble *dieser* oder *jener* Zustände ist, da das Ensemble von der Basiswahl abhängt.

heißt, es ist unmöglich, von dem Messergebnis auf die korrekte Repräsentation $|\psi\rangle \in \mathbb{H}$ vor der Messung schließen. Nichtorthogonale Zustände $\langle\psi_1|\psi_2\rangle \neq 0$ können nicht mit Sicherheit unterschieden werden.

Zweitens ändert der Messprozess den Zustand. Nach der Messung ist die vollständige Information über $|\psi\rangle$ nicht mehr vorhanden und somit auch nicht mehr zugänglich. Wiederholtes Messen am selben System bringt also keinen Informationsgewinn.

Was zunächst nach einer "Unvollkommenheit" der Quantenmechanik aussieht, entpuppt sich bei genauer Betrachtung als intrinsische Eigenschaft der physikalischen Natur. So basiert das "no-cloning" Theorem [11], das besagt, dass es keine Quantenoperation gibt, die beliebige unbekannte Zustände kopiert, auf der Unmöglichkeit, zwei nichtorthogonale Zustände mit Sicherheit zu unterscheiden. Diesem Theorem ist eine ähnlich fundamentale Bedeutung wie der Heisenbergschen Unschärferelation beizumessen.

Vor dem Hintergrund des Kapitels 2.1 können wir den Messvorgang wie folgt interpretieren: Alice kodiert die Information einer Nachricht, indem sie ein physikalisches System in einem bestimmten Zustand präpariert. Zumindest theoretisch kann sie das mit beliebiger Genauigkeit. Dieses System sendet sie zu Bob, der eine Messung daran vornehmen kann, um möglichst viel Information zu extrahieren. In diesem Kapitel beschäftigen wir uns zunächst mit der Frage, wie man den Messprozess formalisieren kann, um dann zu untersuchen, wie viel Information man über ein unbekanntes Qubit prinzipiell erhalten kann und wie viel (klassische) Information mit einem oder mehreren Qubits übermittelt werden kann.

Generalisierte Messungen

Eine ("generalisierte") Messung an $|\psi\rangle \in \mathbb{H}$ kann durch eine Menge $\{E_i\}_{i=1}^m$ von positiven und damit hermiteschen Operatoren¹⁴ auf dem Hilbertraum \mathbb{H} beschrieben werden. Jedes Element E_i steht für ein anderes Messresultat i ($i = 1, \dots, m$). Ferner seien die E_i eine Zerlegung der Eins

$$\sum_{i=1}^m E_i = \mathbf{1}. \quad (2.31)$$

Dann ist $p(i) = \langle\psi|E_i|\psi\rangle$ die Wahrscheinlichkeit für das Ergebnis i . Gl. 2.31 stellt sicher, dass die Summe der Ergebniswahrscheinlichkeiten gleich eins ist, $\sum_i p(i) = 1$.

Diese Formulierung des Messprozesses ist sehr allgemein gehalten; sie gibt uns aber einen sehr eleganten Formalismus in die Hand, um allgemeingültige Aussagen über Resultate von beliebigen, nicht näher zu spezifizierenden, Messungen zu machen. Die Bedeutung der Elemente $\{E_i\}$ wird im Folgenden Abschnitt klarer.

¹⁴genannt POVM-Elemente; POVM steht für engl. "positive operator valued measure".

Projektive Messung

Ein wichtiger Sonderfall der POVM-Messung ist die projektive Messung. Hier sind die Operatoren $E_i := P_i$ orthogonale Projektoren $P_i := |\varphi_i\rangle\langle\varphi_i|$ auf Basisvektoren $|\varphi_i\rangle$, $i \in \{1, \dots, m := \dim \mathbb{H}\}$. Die P_i definieren zusammen mit $a_1, \dots, a_m \in \mathbb{R}$ die Observable M ,

$$M := \sum_{i=1}^m a_i P_i. \quad (2.32)$$

Das i -te Ergebnis tritt im Zustand $|\psi\rangle$ mit Wahrscheinlichkeit $p(i) = \langle\psi|P_i|\psi\rangle = |\langle\varphi_i|\psi\rangle|^2$ auf. Kann man an einem Ensemble von Systemen mit identischen Zuständen ψ viele Messungen durchführen, ergibt sich der Erwartungswert der Observablen in der bekannten Form

$$\langle M \rangle = \langle\psi|M|\psi\rangle = \sum_{i=1}^m a_i |\langle\varphi_i|\psi\rangle|^2 = \sum_{i=1}^m a_i p(i). \quad (2.33)$$

Nach der Messung (mit Resultat i) befindet sich das System im Zustand $\frac{P_i|\psi\rangle}{p(i)} = |\varphi_i\rangle$.

Beispiel

Wir haben bereits drei solcher Observable kennengelernt: die Pauli-Operatoren (Gl. 2.22).

Für z.B. σ_x ist $a_1 = a_P = 1$, $a_2 = a_M = -1$ und $P_1 = P_P$ bzw. $P_2 = P_M$ die Projektoren auf die Basis $\{|P\rangle, |M\rangle\}$. Messen wir die Basiszustände einer konjugierten Basis (vgl. Kap. 2.2.1) – z.B. der Standardbasis –, so ist im Falle $|\psi\rangle = |H\rangle$

$$p(P) = |\langle P|H\rangle|^2 = \frac{1}{2}, \quad p(M) = |\langle M|H\rangle|^2 = \frac{1}{2} \Rightarrow \langle\sigma_x\rangle = 0 \quad (2.34)$$

und genauso für $|\psi\rangle = |V\rangle$

$$p(P) = |\langle P|V\rangle|^2 = \frac{1}{2}, \quad p(M) = |\langle M|V\rangle|^2 = \frac{1}{2} \Rightarrow \langle\sigma_x\rangle = 0. \quad (2.35)$$

Das bedeutet, dass $|H\rangle$ und $|V\rangle$ durch eine Messung in der konjugierten Basis $\{|P\rangle, |M\rangle\}$ vollkommen ununterscheidbar sind (kein Informationsgewinn). In der Standardbasis können sie jedoch wegen $\langle H|H\rangle = \langle V|V\rangle = 1$, $\langle H|V\rangle = 0$ perfekt diskriminiert werden (voller Informationsgewinn).

Unterscheidbarkeit und zugängliche Information

In voller Allgemeinheit kann gezeigt werden, dass zwei nichtorthogonale Zustände $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{H}$, $\langle\psi_1|\psi_2\rangle \neq 0$ nicht fehlerfrei unterschieden werden können.

Dann gäbe es nämlich eine POVM-Messung [7] mit Elementen E_1, E_2, \dots, E_m mit

$$\langle \psi_1 | E_1 | \psi_1 \rangle = \langle \psi_2 | E_2 | \psi_2 \rangle = 1 \quad (2.36)$$

und somit wegen Gl. 2.31

$$\langle \psi_1 | E_{i \neq 1} | \psi_1 \rangle = \langle \psi_2 | E_{i \neq 2} | \psi_2 \rangle = 0. \quad (2.37)$$

Da E_2 hermitesch und positiv ist, gibt es einen hermiteschen Operator $\sqrt{E_2}$ sodass $\sqrt{E_2}^\dagger \sqrt{E_2} = E_2$. Damit gilt

$$0 = \langle \psi_1 | E_2 | \psi_1 \rangle = \langle \psi_1 | \sqrt{E_2}^\dagger \sqrt{E_2} | \psi_1 \rangle = \|\sqrt{E_2} | \psi_1 \rangle\|^2 \Rightarrow \sqrt{E_2} | \psi_1 \rangle = 0 \quad (2.38)$$

Da $\langle \psi_1 | \psi_2 \rangle \neq 0$ kann $|\psi_2\rangle$ in zwei Teile parallel und senkrecht zu $|\psi_1\rangle$ aufgeteilt werden: $|\psi_2\rangle = a |\psi_1\rangle + b |\varphi\rangle$, $|a|^2 + |b|^2 = 1$, $|b| < 1$, $\langle \psi_1 | \varphi \rangle = 0$. Damit ist $\sqrt{E_2} |\psi_2\rangle = b \sqrt{E_2} |\varphi\rangle$ und

$$\langle \psi_2 | E_2 | \psi_2 \rangle = \langle \psi_2 | \sqrt{E_2}^\dagger \sqrt{E_2} | \psi_2 \rangle \stackrel{(2.37)}{=} |b|^2 \underbrace{\langle \varphi | E_2 | \varphi \rangle}_{\leq 1 \text{ wg. Gl. 2.31}} < 1 \quad (2.39)$$

im Widerspruch zur Voraussetzung (Gl. 2.36).

Wie wir gesehen haben 2.2.3, hängt die Informationsmenge, die wir über den Zustand eines quantenmechanischen Systems erhalten können, nicht nur von den Zuständen selbst, sondern auch von der Messung ab. Orthogonale Zustände können durch geschickte Wahl der Observablen optimal, andere (z.B. Gl.2.19) überhaupt nicht unterschieden werden, wenn nur ein einziges Exemplar, also ein einziger Zustand zu Verfügung steht.

In der klassischen Kommunikation tritt dieses Problem nicht auf. Hier gibt es keine prinzipiellen Probleme bei der Unterscheidung der Zustände und deswegen ist die Kapazität $C = \max_{p_X} I(X : Y)$ des Kanals vom Messvorgang unabhängig.

Der Vollständigkeit halber möchte ich noch erwähnen, dass man deswegen in der Quanteninformation die "zugängliche" Information

$$I_{acc}(X : Y) := \max_{\{E_i\}} I(X : Y) \quad (2.40)$$

definiert, wo die $\{E_i\}$ POVM-Elemente sind (vgl. Kap. 2.2.3); sie gibt an, wie viel Information man mit einer Messung, gegeben durch die $\{E_i\}$, aus der Nachricht X maximal ziehen kann. Die Kanalkapazität erhält dann die Form

$$C_Q := \max_{p_X} I_{acc}. \quad (2.41)$$

Bei orthogonalen Zuständen ist $I_{acc}(X : Y) = I(X : Y)$ und damit $C_Q = \max_{p_X} I(X : Y) = C$.

Die Holevo-Schranke

Über einen Kanal, der in klassischen Bits kodierte Information transportiert, kann pro Bit genau 1 bit Information übertragen werden. Dies ist so, da die zwei logischen Zustände (z.B. 0 und 1) des Bit vollkommen unterscheidbar sind. Wie wir gesehen haben, ist diese Unterscheidbarkeit der Zustände bei einem Quantenkanal, über den Information nicht in Bits sondern in Qubits kodiert übertragen wird, nicht mehr unbedingt gegeben. Es stellt sich die Frage, wie viel Information man pro Qubit über einen solchen Quantenkanal maximal transportieren kann. Das nun eingeführte Theorem nach HOLEVO [12] gibt dafür eine obere Schranke an; zum Beweis siehe etwa [7].

Stellen wir uns nun vor, Alice möchte über einen Quantenkanal, also ein quantenmechanisches physikalisches System, Informationen an Bob übertragen. Zu diesem Zweck präpariert sie einen Zustand ρ_X mit der Wahrscheinlichkeit p_X , $X \in \{1, \dots, N\}$, $\sum_i p_i = 1$. Bob bekommt also den gemischten Zustand

$$\rho = \sum_{i=1}^N p_i \rho_i \quad (2.42)$$

und macht eine Messung, die durch die POVM-Elemente (vgl. Kap. 2.2.3) $\{E_Y\}_{Y=1}^m$ gegeben ist. X und Y sind also die Wahrscheinlichkeitsvariablen auf der klassischen Seite von Alice bzw. Bob. Für die gegenseitige Information dieser Größen gilt dann nach HOLEVO

$$I(X : Y) \leq S(\rho) - \sum_{i=1}^N p_i S(\rho_i). \quad (2.43)$$

Dieses Ergebnis kann als Antwort auf die Frage interpretiert werden, wieviel klassische Information (in bit) über ein Quantensystem – z.B. ein oder mehrere Qubits – übertragen werden kann. Ein Beispiel soll dies verdeutlichen:

Beispiel

Betrachten wir das Beispiel aus Gl. 2.30: Da die Zustände $\rho_1 = |H\rangle\langle H|$ und $\rho_2 = |P\rangle\langle P|$ rein sind, ist $S(\rho_1) = S(\rho_2) = 0$ und damit

$$I(X : Y) \leq S(\rho) \approx 0.60 \text{ bit}. \quad (2.44)$$

Die ausgetauschte Information zwischen Alice und Bob kann also nicht größer als ≈ 0.60 bit sein, obwohl zwei "Symbole", nämlich $|H\rangle$ und $|P\rangle$ verwendet werden. Statistisches Rauschen kann die Information noch weiter limitieren.

Allgemein gibt das Theorem in Verbindung mit Gl. 2.27 eine absolute, obere Schranke von

$$I(X : Y) \leq S(\rho) \leq \log \dim \mathbb{H} \quad (2.45)$$

vor. Das heißt, dass durch einen n -Qubit-Zustand (der in einem 2^n – dimensionalen Hilbertraum lebt) nicht mehr als $\log 2^n = n$ bit klassische Information übertragen werden können. Diese obere Schranke wird für reine, orthogonale und gleichverteilte Zustände erreicht:

$$\rho = \sum_{i=1}^N p_i \rho_i = \frac{1}{N} \sum_{i=1}^N |\psi_i\rangle \langle \psi_i| = \mathbf{1}/N. \quad (2.46)$$

Das Ensemble, das ρ beschreibt, ist dann natürlich unabhängig von der Basis (vgl. Kap. 2.2.2) und gleichverteilt.

2.2.4 Verschränkung

Im vorigen Abschnitt haben wir gesehen, dass man mit einem Qubit – genauso wie mit einem Bit – nicht mehr als ein bit Information austauschen kann. Aufgrund der Ununterscheidbarkeit nichtorthogonaler Zustände ist die zugängliche Information sogar im Allgemeinen kleiner.

Wie man recht früh bemerkt hat, ist es genau diese Eigenschaft der Verschränkung, die viele der verblüffendsten und faszinierendsten Phänomene der Quantenmechanik – mit Sicherheit aber der Quanteninformationstheorie – zur Folge hat. Dazu zählen unter anderen die EPR-(Gedanken-) Experimente (siehe unten), die Teleportation [2] von Quantenzuständen, die Quantenkryptographie [13] und das "Quantum Dense Coding" [3].

Aus informationstheoretischer Sicht eröffnen sich völlig neue Arten der Informationskodierung und -prozessierung, die zum Teil effizienter abläuft als es die klassische Physik zulässt.

Hat man n Teilchen vorliegen, von denen jedes einzelne durch einen reinen Zustand im Hilbertraum \mathbb{H}_i , ($i = 1, \dots, n$) repräsentiert wird, so wird der Gesamtzustand¹⁵ $|\Psi^{\otimes n}\rangle$ der n Teilchen im Raum $\mathbb{H}_1 \otimes \mathbb{H}_2 \otimes \dots \otimes \mathbb{H}_n$ dargestellt. Der Zustand heißt separierbar, wenn er sich als tensorielles Produkt von Einteilchenzuständen

$$|\psi^{\otimes n}\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \dots \otimes |\psi\rangle_n \quad (2.47)$$

mit $|\psi\rangle_i \in \mathbb{H}_i$, ($i = 1, \dots, n$) schreiben lässt. Anderenfalls heißt er "verschränkt" [14] oder "nicht separabel". Angenommen, $n = 2$ und die zwei Teilchen implementieren Qubits. Dann kann man sofort die neue kanonische Standardbasis von $\mathbb{H}^{\otimes 2}$ anschreiben¹⁶

$$\mathbb{H}^{\otimes 2} = \text{span}\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\} \quad (2.48)$$

¹⁵Die n Zustände müssen nicht notwendigerweise zu Freiheitsgraden n *verschiedener* Teilchen gehören.

Ein physikalisches Teilchen kann durchaus auch mehrere solcher Zustände (z.B. in verschiedenen Freiheitsgraden wie Spin, energetische Elektronenniveaus, Ort, Impuls, ...) liefern.

¹⁶Benutze häufig auch eine der Kurzformen $|\psi\rangle_A |\varphi\rangle_B := |\psi\rangle |\varphi\rangle := |\psi\varphi\rangle := |\psi\rangle_A \otimes |\varphi\rangle_B$.

und natürlich zwei beliebige Basiszustände unter Berücksichtigung der Normierung superponieren, z.B. zu

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B). \quad (2.49)$$

$|\psi\rangle$ kann nicht mehr in Faktoren $|\varphi\rangle_A \otimes |\varphi\rangle_B$ zerlegt werden. Die zwei Systeme A und B kann man dann nicht mehr unabhängig voneinander als reine Zustände beschreiben. Die Verschränkung ist also zumindest auf dem Papier leicht erzeugt!

In unserem Experiment haben wir es mit verschränkten Zweiteilchensystemen zu tun. Das Konzept der Verschränkung umfasst jedoch Systeme beliebig vieler Teilchen mit diskreten oder kontinuierlichen Freiheitsgraden. Es hat sich gezeigt, dass die Frage, ob ein gegebener – im Allgemeinen gemischter – Zustand ρ separierbar ist, für Systeme mit vielen Freiheitsgraden bzw. Partikeln sehr schwierig zu beantworten ist.

Für die in dieser Arbeit wichtigen reinen Zwei-Qubit Systeme stehen jedoch effiziente Hilfsmittel zur Verfügung (z.B. [15], [16]). Insbesondere kann man maximal verschränkte Zustände definieren, bei denen alle Schmidt-Koeffizienten (siehe z.B. [7]) gleich sind. Sie verletzen die Bell-Ungleichung (siehe unten) *maximal*.

Die Verschränkung von vier Ionen [17] konnte 2000 nachgewiesen werden. Ebenso hat man es geschafft, vier bzw. fünf Photonen miteinander zu verschränken und mit ihrer Hilfe Quantenzustände zu teleportieren [18, 19].

Die Bell-Zustände

Die aus den Elementen der Standardbasis (Gl. 2.49) gebildeten vier symmetrischen Superpositionen

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \quad (2.50)$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \quad (2.51)$$

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \quad (2.52)$$

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \quad (2.53)$$

heißen "Bell-Zustände". Sie sind maximal verschränkt und zeigen perfekte (Anti-) Korrelationen¹⁷. Sie sind außerdem orthogonal und bilden damit ihrerseits eine Basis des vierdimensionalen Zwei-Qubit Raums, die Bell-Basis. Damit sind sie also prinzipiell auch unterscheidbar.

¹⁷korreliert nenne ich zwei Teilchen A und B, wenn man bei Messung beide im gleichen Zustand vorfindet; bei Antikorrelation treten die Zustände genau entgegengesetzt (orthogonal) auf. In der Standardbasis sind $|\Phi^\pm\rangle$ korreliert, die $|\Psi^\pm\rangle$ antikorreliert.

Wenn man die Zustände in einer anderen Basis, z.B. $\{|P\rangle, |M\rangle\}$ misst, ändern sich ihre Korrelationen. Setzt man Gl. 2.19 in Gl. 2.50-2.53 ein, dann erhält man

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|PM\rangle - |MP\rangle) \quad (2.54)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|PP\rangle - |MM\rangle) \quad (2.55)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|PM\rangle + |MP\rangle) \quad (2.56)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|PP\rangle + |MM\rangle). \quad (2.57)$$

Analysiert man die Zustände in dieser Basis, so ergeben $|\Psi^-\rangle$ und $|\Phi^-\rangle$ antikorrelierte Ergebnisse, $|\Psi^+\rangle$ und $|\Phi^+\rangle$ dagegen korrelierte. Die Art der Korrelation zwischen den Ergebnissen einer Messung an den Teilchen hängt also von der gewählten Messbasis ab. Nicht so die Stärke der Korrelationen; wird Teilchen A im Zustand $|P\rangle$ detektiert, so befindet sich Teilchen B *mit Sicherheit* im Zustand $|M\rangle$ (für $|\Psi^-\rangle, |\Phi^-\rangle$) bzw. $|P\rangle$ (für $|\Psi^+\rangle, |\Phi^+\rangle$).

Diese Tatsache, dass die Bell-Zustände abhängig von der Basis unterschiedliche aber stets perfekte Korrelationen aufweisen, werden wir uns bei ihrer Analyse in Kap. 5 zunutze machen.

Das EPR-Paradoxon

Die Korrelationen, die die Bell-Zustände durch die (maximale) Verschränkung erhalten, lassen sich klassisch nicht erklären. Das erstaunlichste daran ist wohl die Tatsache, dass die zwei Teilsysteme A und B – also etwa zwei Photonen – nach ihrer Erzeugung beliebig weit räumlich getrennt werden können, ohne dass sie ihre wechselseitige Beziehung (Korrelation) verlieren. Wird der Zustand eines Teilchens A durch Messung ("Beobachtung") festgelegt, so kollabiert der Gesamtzustand des Systems instantan, sodass eine Messung an B genau das durch die Korrelation bestimmte Ergebnis liefert. Und das auch, wenn die zwei Messungen in so kurzem Abstand hintereinander ausgeführt werden, dass kein Signal mit einer Geschwindigkeit kleiner oder gleich der des Lichts von A nach B gelangen könnte, sie also in diesem Sinne "kausal isoliert" sind.

Im Falle des Bell-Zustands $|\Phi^+\rangle$ zum Beispiel werden stets beide Teilchen bei Projektion auf die Standardbasis im selben Zustand (entweder $|0\rangle$ oder $|1\rangle$) gemessen werden; diese beiden Fälle treten zufällig und mit gleicher Wahrscheinlichkeit auf.

Die Frage, woher das zweite Teilchen B "weiß", welchen Zustand sein sehr weit entfernter Partner A angenommen hat und wie diese Information in beliebig kurzer Zeit beliebig große Distanzen überwinden kann, beschäftigte die Gemüter seit der Entdeckung des Phänomens.

1935 versuchten EINSTEIN, PODOLSKI und ROSEN [1] anhand eines verschränkten Zweiteilchensystems zu zeigen, dass die quantenmechanische Beschreibung nicht vollständig sein kann, weil sie davon ausgingen, dass der Messvorgang am System A den Zustand des Systems B nicht beeinflussen kann. Schließt man also "geisterhafte Fernwirkungen" (Einstein) aus, so müsste jedes der zwei Teilchen, nachdem es vom anderen getrennt wurde, durch lokale Eigenschaften ("Elemente der Realität") beschreibbar sein, die das Messergebnis vollständig determinieren. Da die Quantenmechanik das nicht leistet, schlossen sie, dass die quantenmechanische Beschreibung der Natur unvollständig sei.

Lange Zeit hatte die Frage nach der Vollständigkeit der Quantenmechanik hauptsächlich philosophischen Charakter, da man keine Möglichkeit sah, eine endgültige Entscheidung durch Experimente herbeizuführen. Erst dreißig Jahre später erhielt die Diskussion neue Brisanz, als JOHN BELL einen mathematischen Ausdruck fand [20], der von der Stärke der Korrelationen zwischen den physikalischen Größen zweier Teilchen abhängt; diese Größe¹⁸ S muss der "Bell-Ungleichung" $S \leq 2$ genügen, und zwar in jeder Theorie, in der zwei Voraussetzungen erfüllt sind ("lokaler Realismus"):

1. **Lokalität:** Eine Messung an einem System beeinflusst nicht die Eigenschaften des anderen Systems.
2. **Realität:** Die Eigenschaften jedes Teilchens sind zu jedem Zeitpunkt durch Werte gegeben, die unabhängig von seiner Beobachtung sind.

Diese Theorien werden "local hidden variable theories" (LHV-Theorien) genannt, da die Eigenschaften des Systems lokal und durch (eventuell nicht messbare) versteckte Variable bestimmt sind.

In der selben Arbeit [20] wies BELL darauf hin, dass die Quantenmechanik nur $S \leq 2\sqrt{2}$ fordert und die obere Grenze für den von BOHM vorgeschlagenen Spin-Singlett Zustand (das ist der verschränkte Zustand Gl. 2.50, auch "EPR-Paar" genannt) angenommen wird¹⁹. Solche Zustände werden maximal verschränkt genannt, da sie die Ungleichung $S \leq 2$ maximal verletzen.

Tatsächlich fanden unter anderen FREEDMAN und CLAUSER 1972 [21] starke experimentelle Hinweise²⁰, dass die Korrelationen der von ihnen verwendeten verschränkten Photonenpaare aus Calcium-Kaskadenemission die Bell-Ungleichung verletzen, dass es also in der Natur Zustände gibt, die einer Korrelationsstatistik gehorchen, die in keiner LHV-Theorie möglich ist.

ASPECT ET. AL. führten zahlreiche und sehr umfassende experimentelle Studien (z.B. [22, 23]) zu den nichtklassischen Korrelationen der Verschränkung durch.

¹⁸Nicht zu verwechseln mit der von Neumann Entropie aus Gl. 2.25.

¹⁹Tatsächlich verletzen ausschließlich verschränkte Zustände – wenn auch nicht alle – die Bell-Ungleichung. Die Messungen zur Verletzung der Bell-Ungleichungen sind vom Zustand abhängig.

²⁰Auch in ihren Experimenten gab es anfechtbare Annahmen, siehe unten.

Es sei erwähnt, dass die bis dato durchgeführten Experimente zur Verletzung der Bell-Ungleichung aufgrund experimenteller Imperfektionen noch nicht *zwingend* jede LHV-Theorie ausschließen konnten. Es konnten in letzter Zeit in mehreren Experimenten verschiedene dieser "Hintertürchen" geschlossen werden, so konnten z.B. WEIHS ET AL. mit polarisationsverschränkten Photonen unter streng lokalen Bedingungen (keine Wechselwirkung im Rahmen der speziellen Relativitätstheorie möglich) eine Bell-Ungleichung²¹ verletzen [25]. ROWE ET AL. führten Experimente [26] mit sehr hoher Detektionseffizienz an Ionen durch und konnten damit das so genannte "detection loophole" schließen²².

Ein Experiment, das sowohl den Austausch von Signalen bzw. Wechselwirkungen ausschließt *und* eine ausreichende Detektionseffizienz beinhaltet lässt noch auf sich warten. Mögliche Kandidaten könnten Versuche an "Hybridsystemen" sein, bei denen weit entfernte, einzelne Atome (oder Ionen) in Fallen (hohe Detektionseffizienz) zunächst mit Photonen verschränkt werden, welche die große Distanz zwischen den massiven Teilchen zurücklegen können. Danach kann die Verschränkung durch Messung²³ an den Photonen auf die Atome übertragen werden.

Die Ion-Photon Verschränkung konnte kürzlich erzeugt und nachgewiesen werden [27]. Damit hat man es auch erstmals geschafft, die Information eines Quantenkanals – repräsentiert durch das Photon, das die Information über große Distanzen transportieren kann – auf das als "Quantenspeicher" fungierende Ion zu übertragen²⁴.

Mit der Schließung aller experimentellen "Hintertürchen" könnte man auf einen Schlag eine ganze Klasse von Theorien widerlegen und zeigen, dass die Beschreibung der Natur durch die Quantenmechanik in diesem Sinne korrekt ist.

Es ist ein noch nicht endgültig verstandenes Problem, inwieweit und in welcher Form eine oder beide der zwei oben genannten Voraussetzungen – Lokalität und Realität – nicht erfüllt sein könnten.

Lokale Operationen auf einem Bell-Zustand

Die Verschränkung in einem System bleibt unter lokalen unitären Operationen und klassischer Kommunikation (LOCC) erhalten[7]. Verschränkung kann also als eine im ab-

²¹In diesen wie in den meisten folgenden Versuchen zur lokalen Realität verwendete man eine besser auf die experimentellen Bedürfnisse angepasste Ungleichung nach CLAUSER, HORNE, SHIMONY UND HOLT [24]

²²Bei nicht hundertprozentiger Detektionswahrscheinlichkeit ist es im Prinzip möglich, dass zwar das Ensemble der detektierten Teilchen die Bell-Ungleichung verletzt, jedoch alle (detektierten und verloren gegangenen) zusammen dies nicht tun.

²³hierzu wäre eine vollständige Bell-Projektion nötig, also eine projektive Messung in der Basis der Zustände 2.50-2.53. Siehe dazu auch Kap. 5.

²⁴Dass die Korrelationen über große Distanzen bestehen können, zeigten TITTEL ET AL. durch den Nachweis von Energie-Zeit-Verschränkung (siehe Kap. 5.4) von weit entfernten (10 km) Photonenpaaren [28] im Jahr 1998.

geschlossenen System konstante Ressource angesehen werden. Vermindert man die Verschränkung in einem Teilsystem, so muss sie in einem anderen Teilsystem anwachsen. Für ein Zweiteilchensystem wie die Bell-Zustände hat das zur Folge, dass eine Operation $U_A \otimes \mathbb{1}_B$ den Grad der Verschränkung nicht verändern kann. Es werden also nur maximal verschränkte auf andere maximal verschränkte Vektoren abgebildet. Wendet man auf eines – sei es das erste – der Teilchen im Zustand $|\Psi^-\rangle$ (Gl. 2.50) eine allgemeine unitäre Operation (vgl. Kap. 2.2.1) der Form

$$U(\theta, \alpha, \beta) \doteq \begin{pmatrix} e^{i\alpha} \cos \frac{\theta}{2} & ie^{i\beta} \sin \frac{\theta}{2} \\ ie^{-i\beta} \sin \frac{\theta}{2} & e^{-i\alpha} \cos \frac{\theta}{2} \end{pmatrix} \quad \text{wo } \theta \in [0, \pi] \quad \alpha, \beta \in [0, 2\pi[\quad (2.58)$$

an, so sind die dadurch generierbaren Zustände $|\Psi\rangle$ gegeben durch

$$|\Psi\rangle = \frac{\cos \frac{\theta}{2}}{\sqrt{2}} (e^{i\alpha} |01\rangle - e^{-i\alpha} |10\rangle) - i \frac{\sin \frac{\theta}{2}}{\sqrt{2}} (e^{i\beta} |00\rangle - e^{-i\beta} |11\rangle), \quad (2.59)$$

mit den drei reellen Paramtern θ, α, β . Interessanterweise sind darunter – bis auf globale Phasen, die ich ich der Vollständigkeit halber mit angeschrieben habe – auch die drei anderen Bell-Zustände:

$$\begin{aligned} U(0, 0, \beta) : |\Psi^-\rangle &\mapsto |\Psi^-\rangle \\ U(0, \frac{\pi}{2}, \beta) : |\Psi^-\rangle &\mapsto i|\Psi^+\rangle \\ U(\pi, \alpha, 0) : |\Psi^-\rangle &\mapsto -i|\Phi^-\rangle \\ U(\pi, \alpha, \frac{\pi}{2}) : |\Psi^-\rangle &\mapsto |\Phi^+\rangle. \end{aligned} \quad (2.60)$$

Damit wird auch klar, dass die Zustände (2.59) eine Teilmenge, nicht aber einen Teilraum des Zwei-Qubit Hilbertraums bilden [3]. Zum Beispiel ist der Produktzustand $(|\Phi^-\rangle + |\Phi^+\rangle)/\sqrt{2} = |00\rangle$ nicht darunter.

Gleichung 2.60 fasst die wichtige Aussage zusammen, dass man – ausgehend von $|\Psi^-\rangle$ – alle vier orthogonalen Bell-Zustände erzeugen kann, indem man auf auf ein *einziges* Teilchen eine von vier Transformationen anwendet²⁵. Dagegen kann eine lokale Operation $U_A \otimes \mathbb{1}_B$ auf einem Zwei-Qubit Produktzustand $|A\rangle \otimes |B\rangle$, z.B. einem Element der Standardbasis in $\mathbb{H}^{\otimes 2}$, trivialerweise nicht alle dazu orthogonalen Zustände erzeugen. Es ist genau diese Eigenschaft der Verschränkung, auf der das Dense Coding beruht.

²⁵Es ist klar, dass dies mit entsprechenden Operationen auch für jeden anderen Bell-Anfangszustand zutrifft, da man jeden Zustand zunächst mittels $[U(\theta, \alpha, \beta)]^\dagger = U(-\theta, -\alpha, \beta)$ auf $|\Psi^-\rangle$ abbilden kann.

3 Superdichtes Quantenkodieren

3.1 Einführung

Im Jahr 1992 stellten BENNETT und WIESNER [3] ihr Protokoll zum *Dense Coding*¹ vor, bei dem es um die Übertragung von klassischer Information über einen Quantenkanal – implementiert durch Zwei-Qubit-Systeme – geht. Es stellt einen Meilenstein in der Geschichte der damals noch sehr jungen Quanteninformatik dar. Es zeigt bei aller konzeptionellen Einfachheit die verblüffenden Eigenheiten der quantalen Informationsrepräsentierung in verschränkten Systemen und ihre klassisch nicht erklärbaren Konsequenzen.

Im Folgenden werde ich zunächst einmal den schematischen Ablauf des "superdichten Kodierens" festlegen und den Widerspruch zur klassischen Physik aufzeigen. Dafür benötigen wir die Resultate, die in den vorigen Abschnitten dargelegt wurden.

Danach möchten wir kurz analysieren, welche Möglichkeiten das Protokoll bietet und welche Grenzen es hat, beziehungsweise was mit dem superdichten Kodieren *nicht* möglich ist – nämlich superluminare ("schneller als das Licht") Informationsübertragung.

3.2 Das Protokoll

Die Grundidee beim Dense Coding ist, dass sich die zwei Parteien Alice und Bob ein EPR-Paar teilen (vgl. Abb 3.1). Alice kann dann durch eine Operation auf ihrem Teilchen einen der vier Bell-Zustände erzeugen. Danach schickt sie Bob ihr Teilchen wieder zu. Bob führt dann auf beiden Teilchen eine Messung zur Unterscheidung der vier Bell-Zustände durch und erhält dadurch *zwei* bit klassische Information von Alice, obwohl nur *ein* Qubit zwischen den beiden ausgetauscht worden ist.

3.2.1 Ablauf

In Abb. 3.1 ist der Ablauf der Informationsübertragung von Alice zu Bob schematisch dargestellt. Das Protokoll sieht folgende Schritte vor:

¹Engl. auch "(super)dense coding", "quantum dense coding"; dt. "superdichtes Quantenkodieren".

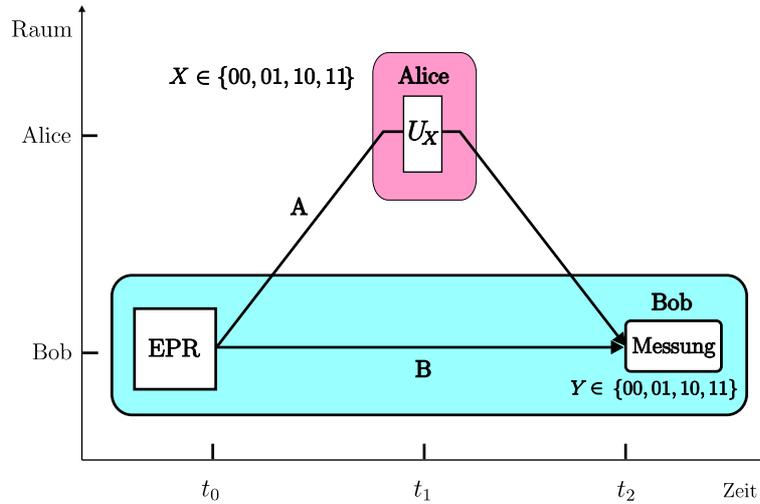


Abbildung 3.1: Schematischer Ablauf des Dense Coding Protokolls. Ein EPR-Paar wird erzeugt, zum Zeitpunkt t_0 getrennt und jeweils ein Teilchen zu Alice bzw. Bob geschickt. Alice manipuliert nur ihr Teilchen und schickt es daraufhin wieder zu Bob. Dieser misst den Gesamtzustand.

1. Die zwei Teilchen einer EPR-Quelle werden zum Zeitpunkt t_0 an die zwei Parteien Alice (Sender) und Bob (Empfänger) verteilt. Jeder der beiden ist also im Besitz eines *einzigsten* Teilchens A bzw. B.
2. Alice wählt zum Zeitpunkt t_1 $X \in A_X := \{00, 01, 10, 11\}$ und damit eine der vier unitären Transformationen U_X :

$$\begin{aligned}
 U_{00} &:= \mathbb{1} & \doteq & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
 U_{01} &:= \sigma_z & \doteq & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
 U_{10} &:= -\sigma_x & \doteq & \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \\
 U_{11} &:= -i\sigma_y & \doteq & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
 \end{aligned} \tag{3.1}$$

aus, wendet sie lokal auf ihr Teilchen A an und präpariert somit einen der Bell-Zustände (vgl. Gl. 2.50-2.53)

$$\begin{aligned}
 |\Psi_{00}\rangle &:= |\Psi^-\rangle & = & (U_{00} \otimes \mathbb{1}) |\Psi^-\rangle \\
 |\Psi_{01}\rangle &:= |\Psi^+\rangle & = & (U_{01} \otimes \mathbb{1}) |\Psi^-\rangle \\
 |\Psi_{10}\rangle &:= |\Phi^-\rangle & = & (U_{10} \otimes \mathbb{1}) |\Psi^-\rangle \\
 |\Psi_{11}\rangle &:= |\Phi^+\rangle & = & (U_{11} \otimes \mathbb{1}) |\Psi^-\rangle
 \end{aligned} \tag{3.2}$$

3. Das Teilchen A wird von Alice zu Bob geschickt.
4. Bob führt an *beiden* Teilchen A und B eine Projektions-Messung durch, die ganz formal durch die POVM-Elemente $\{E_i\}_{i=1}^4 =: \{E_Y\}$, $Y \in A_Y := \{00, 01, 10, 11\}$ dargestellt werden kann, um die vier Zustände aus Gl. 3.2 zu unterscheiden. Y ist das Ergebnis der Übertragung.

3.2.2 Erläuterungen

Der erste Schritt besteht in der Präparation des Anfangszustands und der Trennung der Einzelsysteme, wobei die Distanz zwischen den Systemen sehr groß sein kann.

Normalerweise wird an dieser Stelle der EPR-Zustand $|\Psi^-\rangle$ verwendet [3]. Es macht jedoch keinen grundsätzlichen Unterschied, wenn man einen der anderen maximal verschränkten Zustände aus Gl. 2.59 verwendet, da ja jeder dieser Zustände lokal in $|\Psi^-\rangle$ transformiert werden kann.

Wir wollen annehmen, dass Bob bei der Quelle bleibt und Alice weit weg von ihr ist. Da die einzelnen Teilchen maximal mit Lichtgeschwindigkeit zu Alice bzw. Bob propagieren können, impliziert diese Annahme, dass auch die Zeitspanne $\tau := t_1 - t_0$ zwischen der Entstehung der Teilchen und dem zweiten Schritt keinerlei Beschränkung unterliegt. Die Parteien können ihre Teilchen auch "speichern". Die Geschwindigkeit von Teilchen A spielt also keine prinzipielle Rolle in diesem Protokoll, auch wenn sie in der vorliegenden Arbeit gleich der Lichtgeschwindigkeit ist.

Danach kodiert Alice die Information, indem sie aus dem Anfangszustand einen der vier Bell-Zustände *lokal* generiert². Wie wir im Abschnitt 2.2.4 sahen, ist Schritt 2 tatsächlich möglich. Die dort angegebenen Operatoren sind bis auf unerhebliche globale Phasen identisch mit den hier definierten. Auf Bobs Teilchen wird nicht operiert, es bleibt unangetastet.

Da wir angenommen haben, dass Bob bei der Quelle bleibt, findet der einzige physikalische "Teilchentransfer" durch Teilchen A in Schritt eins von der Quelle zu Alice und in Schritt drei von Alice zu Bob statt. Es existiert daneben kein anderer klassischer oder quantaler Kanal, durch den Information übertragen werden könnte.

Zum Beispiel kann man sich eine Implementierung mit Photonen und minimalen Wegstrecken zwischen Alice und Bob vorstellen, sodass im Rahmen der speziellen Relativitätstheorie kein anderes Signal schneller als das Photon A Information zwischen Alice und Bob (oder der Quelle) transportieren kann.

Die Annahme, dass Bob bei der Quelle verbleibt, dient ausschließlich der Anschaulichkeit. Wir könnten sogar zulassen, dass die Quelle nach der Emission zerstört wird.

Wenn Bob im Besitz beider Teilchen ist, muss er nur noch die Messung durchführen,

²"lokal" heißt natürlich, dass der Zustand eine Transformation $U_A \otimes \mathbb{1}_B$ erfährt.

die die Zustände unterscheidet. Dies ist *grundsätzlich* möglich, da die vier Bell-Zustände orthogonal sind.

3.2.3 Informationsübertragung beim Dense Coding

Das überraschende Ergebnis des Dense-Coding Protokolls ist, dass Alice 2 bit klassische Information an Bob übertragen konnte, obwohl sie nur ein einziges Qubit mit ihm ausgetauscht hat. In Kap. 2.2.3 haben wir jedoch gesehen, dass ein Qubit maximal 1 bit Information transportieren kann!

Beim superdichten Kodieren haben wir angenommen, dass an den Teilchen A und B keine Dekohärenz und auch keine unitäre Störung – man könnte also sagen: kein Rauschen – auftritt. Dann misst Bob nämlich genau den Bellzustand, den Alice zuvor erzeugt hatte. Jede Transformation X löst also das richtige Messergebnis Y aus.

Wir können somit die Transfermatrix $p(Y = y|X = x)$ mit $x \in A_X$ und $y \in A_Y = A_X = \{00, 01, 10, 00\}$ für die *klassischen* Variablen X und Y diagonal schreiben. Nach Gl. 2.12 hängt die gegenseitige Information dann nur noch von der Quellenverteilung p_X ab. Durch geeignete Kodierung (das bedeutet Gleichverteilung $p_X \equiv \frac{1}{4}$, vgl. Gl. 2.8 und 2.4) kann Alice $H(X) = \log |A_X| = 2$ bit erreichen. Damit ist gleichzeitig die Kapazität (Gl. 2.13) des Kanals zu

$$C(X : Y) = \max_{p_X} I(X : Y) = 2 \text{ bit} \quad (3.3)$$

gegeben.

Ich möchte noch darauf hinweisen, dass Gl. 3.3 tatsächlich die obere Grenze darstellt, die man durch das Dense Coding erreichen kann. Würde man zum Beispiel statt der Bell-Zustände auf andere, nichtorthogonale Zustände ausweichen, so wäre die zugängliche Information I_{acc} und damit auch die Kapazität reduziert (vgl. Gl. 2.41 und 2.40).

Es gäbe dann stets eine endliche Wahrscheinlichkeit, dass ein Zustand falsch identifiziert würde (vgl. Kap. 2.2.3).

Das Ergebnis aus Gl. 3.3, $C = 2$ bit, sieht nach einem Widerspruch zu der in Kap. 2.2.3 angegebenen Schranke nach aus; der Satz nach HOLEVO besagt, dass man mit einem Qubit, das Alice zu Bob sendet, maximal 1 bit klassische Information übertragen kann!

Dieser Widerspruch löst sich auf, wenn man bedenkt, dass Bob tatsächlich an *beiden* Teilchen messen muss, um die vollen 2 bit Information zu erhalten. Wäre das nicht so, ergäbe sich tatsächlich eine Inkonsistenz.

3.3 Einteilchenstatistik der Bell-Zustände

3.3.1 Reduzierte Dichteoperatoren

Der quantenmechanische Zustand eines Teilchens, das Teil eines Mehrteilchensystems ist, wird durch den reduzierten Dichteoperator beschrieben. Den Dichteoperator ρ_A eines einzelnen Teilchens A, das Teil eines Bell-Zustands ist, erhält man dementsprechend, indem man die gesamte Dichtematrix ρ_{Bell} über die Basiszustände des Teilchens B spurt:

$$\rho_A = \text{tr}_B\{\rho_{Bell}\} = \sum_{i=0,1} \langle i|_B \rho_{Bell} |i\rangle_B = \frac{1}{2}\mathbb{1} \quad (3.4)$$

Das Ergebnis $\rho_A = \frac{1}{2}\mathbb{1}$ ergibt sich für beide Teilchen A und B, also $\rho_A \equiv \rho_B$, und für jeden³ der vier Bell-Zustände

$$\rho_{Bell} \in \{\rho_{\Psi^-}, \rho_{\Psi^+}, \rho_{\Phi^-}, \rho_{\Phi^+}\}, \quad (3.5)$$

Die zugehörigen Dichtematrizen in der Zwei-Qubit Standardbasis $\{|HH\rangle, |HV\rangle, |VH\rangle, |VV\rangle\}$ lauten

$$\rho_{\Psi^-} = |\Psi^-\rangle \langle \Psi^-| \doteq \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (3.6)$$

$$\rho_{\Psi^+} = |\Psi^+\rangle \langle \Psi^+| \doteq \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (3.7)$$

$$\rho_{\Phi^-} = |\Phi^-\rangle \langle \Phi^-| \doteq \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \quad (3.8)$$

$$\rho_{\Phi^+} = |\Phi^+\rangle \langle \Phi^+| \doteq \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad (3.9)$$

Die Einteilchenzustände der Bell-Zustände sind also vollständig gemischt ($\propto \mathbb{1}$), während der zugehörige Zweiteilchenzustand rein ist! Dies ist eine spezielle Eigenschaft der Verschränkung; wegen Gl. 2.27 gilt für die von Neumann-Entropien des Gesamt- bzw. der Teilsysteme A und B

$$0 = S(\rho_{Bell}) \leq S(\rho_{A/B}) = 1, \quad (3.10)$$

³Tatsächlich gilt dies sogar für alle Zustände aus Gl. 2.59, also für alle lokalen unitären Transformationen $U_A = U(\theta, \alpha, \beta)$ aus Gl. 2.58 von Alice.

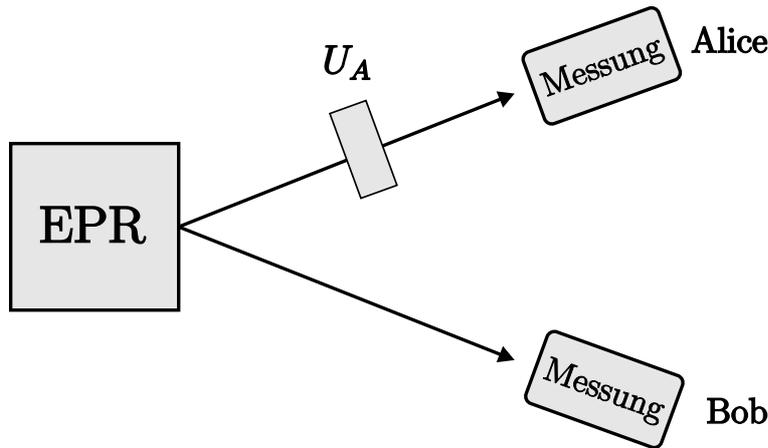


Abbildung 3.2: Alice und Bob teilen sich ein EPR-Paar im Zustand $|\psi^-\rangle$. Alice macht eine beliebige unitäre Operation auf ihrem Qubit; trotzdem ist sowohl Alices als auch Bobs Einteilchenzustand, an dem sie jeweils messen können, stets der selbe.

da die Eigenwerte von $\rho_{A/B}$ gleich $\lambda_1 = \lambda_2 = \frac{1}{2}$ sind (Gl. 2.25). Das bedeutet, dass die Entropie des Gesamtsystems kleiner ist als die Summe der Entropien seiner Einzelsysteme (so genannte "Subadditivität"). Die Entropie eines Produktzustandes ist dagegen gleich der Summe der Entropien seiner Teile.

3.3.2 Lokale Messungen

Das Resultat aus Gl. 3.4 hat zentrale Bedeutung für den Kommunikationsprozess zwischen Alice und Bob.

Wenn Bob nur an seinem eigenen Teilchen misst (Abb. 3.2), sieht er nur den Zustand mit Dichtematrix $\rho_B = \mathbb{1}/2$, der für *alle* von Alice präparierten Bell-Zustände gleich ist, und erhält so keine Information darüber, welche Operation U_X Alice gewählt hat. Formal folgt das aus Gl. 2.43 mit $p_i = \frac{1}{4}$, $\rho_i = \mathbb{1}/2$, ($i = 1, \dots, 4$)

$$I(X : Y) \leq S\left(\frac{1}{4}(\mathbb{1}/2 + \mathbb{1}/2 + \mathbb{1}/2 + \mathbb{1}/2)\right) - \frac{1}{4} \cdot 4 \cdot S(\mathbb{1}/2) = 0. \quad (3.11)$$

Es ist auch leicht zu zeigen, dass *jede* lokale Messung von Bob an seinem Teilchen das selbe Resultat hat, egal, welche Operation Alice auf ihrem Teilchen gemacht hat. Mit anderen Worten, $\langle \Psi | \mathbb{1} \otimes E | \Psi \rangle$ ist unabhängig von $|\Psi\rangle \in \{|\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Phi^+\rangle\}$ für jeden positiven Operator E (vgl. Kap. 2.2.3).

Damit kann Bob mit keiner Messung Information aus seinem Teilchen allein erhalten. Das ist sehr interessant, da es zeigt, dass die Information in einem maximal verschränkten Zustand sozusagen vollständig über das System verteilt ist, oder besser ausgedrückt:

Die Information ist nicht in den individuellen Eigenschaften der Einzelteilchen, sondern ausschließlich in ihren (perfekten) Korrelationen kodiert.

3.4 Diskussion

Bob kann also weder durch *irgendeine* lokale Messung Information über Alices Wahl von X erhalten, noch kann Alice durch *irgendeine* lokale unitäre Operation beeinflussen, was Bob an seinem Teilchen misst. Damit reicht die Verschränkung zwischen den zwei Teilchen/Parteien allein nicht aus, um Information zwischen ihnen auszutauschen. Die Information wird vollständig von Alice zum Zeitpunkt t_1 in das System kodiert.

Damit ist auch keine Signalübermittlung mit Überlichtgeschwindigkeit möglich. Um Information zu erhalten, muss Bob nämlich stets eine gemeinsame Messung an beiden Teilchen durchführen; dazu muss ein Teilchen (A) den Weg zwischen Alice und Bob tatsächlich zurücklegen, was es natürlich nicht schneller als das Licht kann.

Berücksichtigt man, dass tatsächlich beide Teilchen in den Vorgang des Dense Coding involviert sein müssen, so ist natürlich die Holevo-Schranke ("maximal 2 bit mit 2 Qubits") durch die Übertragung von 2 bit klassischer Information nicht verletzt.

Darüber hinaus muss der Quantenkanal zwischen Alice und Bob tatsächlich zweimal benutzt werden, einmal von Bob zu Alice beim ersten Schritt des Protokolls und ein zweites Mal beim Zurücksenden zu Bob. Ohne die zweimalige Verwendung dieses (oder eines anderen) Kanals könnten die zwei Parteien die für das Protokoll notwendige "Resource" der Verschränkung nicht teilen. Klassische Information wird dabei durch den vollständig gemischten Einteilchenzustand jedoch nicht übertragen.

Das aus klassischer Sicht verblüffende am Dense Coding ist somit nicht in erster Linie, dass Alice 2 bit Information durch das Versenden eines einzelnen Qubits übertragen kann. Es ist vielmehr die Art und Weise, in der die Information in dem maximal verschränkten Zustand kodiert wird.

Eine Interpretation nach SCHUMACHER [3, 29] ist, dass ein bit Information von (Alice, t_1) nach (Bob, t_2) vorwärts in der Zeit über Alices (manipuliertes) Qubit transmittiert wird, das andere bit jedoch von (Alice, t_1) ebenfalls auf ihrem Qubit in der Zeit *rückwärts* zur Quelle (Bob, t_0) läuft, um dann vorwärts in der Zeit über Bobs Teilchen ebenfalls zu (Bob, t_2) zu gelangen⁴. Dort ergeben sie zusammen die gesamte Nachricht mit 2 bit Information.

Das Phänomen der Verschränkung zwischen – möglicherweise weit entfernten – Teilchen zwingt uns in jedem Fall, unsere Vorstellung über die "Eigenschaften" eines quantalen

⁴Hier gilt das bereits erwähnte, nämlich dass es nicht erheblich ist, dass Bob bei der Quelle bleibt (oder umgekehrt).

Systems zu überdenken. Auf jeden Fall sollte man erkennen, dass Alice durch ihre unitäre Operation eben nicht ein einzelnes Teilchen, sondern das ganze System *an* einem seiner Teile verändert.

Zur Realisierung des Dense Codings mit polarisationskodierten Qubits benötigen wir also dreierlei:

1. Eine Quelle für maximal verschränkte Photonenpaare.
2. Eine Implementierung der lokalen unitären Operationen auf Alices Photon, um aus dem Anfangszustand die vier Bell-Zustände zu präparieren.
3. Die Unterscheidung der vier Bell-Zustände durch Bob, also die Dekodierung des quantalen Systems in eine klassische Form der Informationsdarstellung.

Die Dekodierung der Information aus den Bell-Zuständen ist dabei ebenso essentiell wie die Generierung beziehungsweise der Austausch des *maximal verschränkten* Paares. Wie wir gesehen haben, ist es ja gerade die Verschränkung, die die Kodierung der 2 bit Information durch lokale Transformation möglich macht.

Dementsprechend muss die Information, die in den nichtklassischen Korrelationen steckt, durch die Messung ausgelesen werden können. Dieser Schritt der Dekodierung ist nicht trivial, weil er die Projektion maximal verschränkter Zustände auf eine Produktbasis darstellt.

Wie ich in Kap. 5 genauer darlegen werde, ist diese Aufgabe mit "normalen" Mitteln, nämlich passiven linearoptischen Elementen, nicht effizient lösbar. Die vollständige Bell-Zustandsunterscheidung ist damit aus experimenteller Sicht die größte Herausforderung in dieser Arbeit.

4 Erzeugung der verschränkten Zustände

Inhalt

4.1 Einführung	42
4.2 Spontane parametrischen Fluoreszenz	43
4.2.1 Theorie der Konversion	43
4.2.2 Räumliche Verteilung der Emissionsmoden	44
4.2.3 Die Photonenpaarquelle	45
4.3 Zur Detektion der Einzelphotonen	49
4.4 Die Spektren der Einzelphotonen	51
4.5 Die Polarisationsverschränkung	53
4.5.1 Transformation des Quellenzustands	53
4.5.2 Die Polarisationskorrelationen	54

4.1 Einführung

Wie wir in Kap. 3 gesehen haben, beruht das Dense Coding auf den stark nichtklassischen Korrelationen, die maximal verschränkte Zweiteilchenzustände aufweisen. In diesem Kapitel beschreibe ich den Mechanismus, den ich zur Erzeugung von polarisationsverschränkten Photonenpaaren verwende, die *spontane parametrische Fluoreszenz*¹ (SPF).

Danach werde ich zeigen, wie unter Ausnutzung dieses Mechanismus eine sehr kompakte und effiziente Quelle für verschränkte Photonen konstruiert werden konnte. Da der Prozess zur Verschränkungserzeugung – die spontane Konvertierung eines Photons in zwei Tochterphotonen in nichtlinearer Umgebung – sehr ineffizient im Vergleich zu linearen

¹engl. "spontaneous parametric down conversion", kurz SPDC

Prozessen geschieht, lag das Hauptaugenmerk bei der Konzipierung der Quelle auf der Maximierung der Ausbeute.

Mit dieser Art der Quelle kann man Photonenpaare herstellen, die in mehr als einem Freiheitsgrad verschränkt sind. Tatsächlich werden wir uns diesen Umstand zunutze machen, um die vollständige Zustandsanalyse an den Bell-Zuständen durchführen zu können (Kap. 5. Dabei nutzen wir neben der Polarisationsverschränkung die Korrelationen in Energie beziehungsweise Zeit aus. In Kap. 5.4 werde ich auf den Ursprung dieser Art der Verschränkung genauer eingehen.

4.2 Spontane parametrischen Fluoreszenz

4.2.1 Theorie der Konversion

Die durch ein einfallendes elektromagnetisches Feld $\vec{E} = (E^1, E^2, E^3)^T$ in einem dielektrischen Medium induzierte makroskopische elektrische Polarisation $\vec{P} = (P^1, P^2, P^3)^T$ ist im Allgemeinen nichtlinear von der Feldstärke $d\vec{E}$ abhängig. In tensorieller Schreibweise ist die Polarisation gegeben durch

$$P^i = \epsilon_0 \left(\sum_j \chi_{ij}^{(1)} E^j + \sum_{j,k} \chi_{ijk}^{(2)} E^j E^k + \sum_{j,k,l} \chi_{ijkl}^{(3)} E^j E^k E^l + \dots \right). \quad (4.1)$$

Der Tensor $(n+1)$ -ter Stufe $\chi^{(n)}$ heißt Suszeptibilität n -ter Ordnung und modelliert die Stärke der Antwort des Mediums auf das Feld. Die Antwort ist die elektrische Polarisation und entsteht durch räumliche Mittelung über induzierte mikroskopische (atomare, molekulare) Dipolmomente. Es gilt $\chi^{(n+1)} \ll \chi^{(n)}$, ($n \geq 1$), die höheren Terme sind also stark unterdrückt und nur für hohe Feldintensitäten beobachtbar, wie sie etwa ein starker Laser erzeugt.

Phänomene, die auf den höheren Termen $n \geq 2$ beruhen, heißen nichtlineare optische Phänomene (z.B. Drei- und Vierwellenmischen aufgrund von Nichtlinearitäten zweiter und dritter Ordnung). Für hinreichend schwache Felder ist $\vec{P} = \epsilon_0 \chi^{(1)} \vec{E}$, woraus die linearen optischen Effekte wie Absorption, Brechung oder Dispersion folgen. Die Größen $\chi^{(2n)}$ gerader Ordnung können nur von null verschieden sein, wenn die Kristallstruktur des Mediums nicht symmetrisch bezüglich Inversion (Spiegelung am Ursprung) ist.

Gehen wir davon aus, dass wir Beiträge jenseits von $\chi^{(2)}$ vernachlässigen können und \vec{E} eine ebene Welle der Frequenz² ω_p darstellt, dann sieht man, dass der quadratische Term zwei neue Felder \vec{E}_1, \vec{E}_2 mit Frequenzen $\omega_1, \omega_2 \leq \omega_p$ darstellt. Eine quantenmechanische Untersuchung des Vorgangs ist z.B. in [30, 31, 32, 33] gegeben. Danach stellt sich der

²Genau genommen ist die Frequenz $\nu = 2\pi \cdot \omega$; unterscheide dies aber sprachlich nicht.

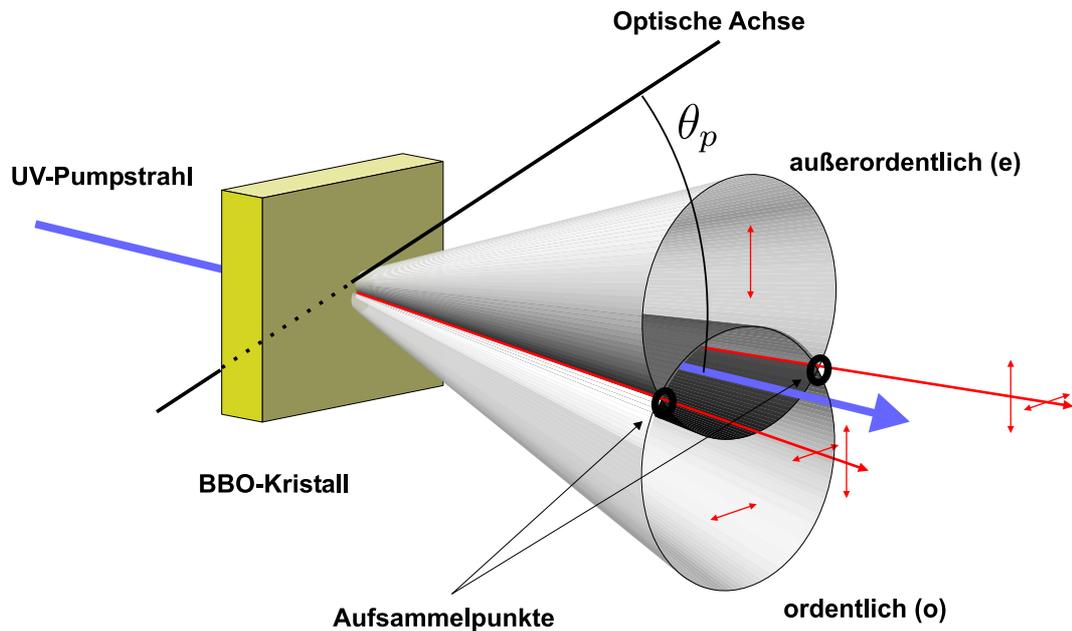


Abbildung 4.1: Die zwei Emissionskegel der spontanen parametrischen Fluoreszenz vom Typ II.

Prozess folgendermaßen dar: Ein Pumpphoton des einfallenden Feldes wechselwirkt mit dem nichtlinearen Medium und konvertiert dabei spontan in zwei Tochterphotonen³ unter Energie- und Impulserhaltung

$$\begin{aligned}\omega_1 + \omega_2 &= \omega_p \\ \vec{k}_1 + \vec{k}_2 &= \vec{k}_p.\end{aligned}\quad (4.2)$$

Dieser Vorgang ist klassisch verboten, da *beide* Tochterphotonen bei dem Prozess spontan entstehen und nicht etwa eines von ihnen den Prozess stimuliert. Man beachte auch, dass der "Zerfall" eines (masselosen) Photons im Vakuum verboten ist. Die Doppelbrechung im nichtlinearen Kristall und die damit verbundenen unterschiedlichen Brechungsindizes für den außerordentlich polarisierten Pumpstrahl ermöglichen jedoch den Prozess. Die Wellenvektoren in Gl. 4.2 sind deswegen vom Winkel zur optischen Achse sowie von der Wellenlänge der Photonen abhängig.

4.2.2 Räumliche Verteilung der Emissionsmoden

Bei Typ II SPF ist eines der spontan konvertierten Photonen ordentlich, das andere außerordentlich zur optischen Achse des Kristalls polarisiert. Wegen der doppelbrechenden

³Auch "signal" und "idler" genannt.

Eigenschaft des Kristalls verlassen Photonen gleicher Energie ($\omega_1 = \omega_2 = \omega_p/2$, so genannte "entartete" Fluoreszenz) den Kristall daher auf zwei verschiedenen Kegelmänteln, aber wegen der Impulserhaltung symmetrisch um die Pumprichtung (siehe Abb. 4.1).

Die zwei Kegel haben den gleichen Öffnungswinkel, sind aber jeweils um den Winkel $\pm\theta$ gegen den Pumpstrahl geneigt.

Diesen Winkel kann man in einem weiten Bereich variieren, indem man den Winkel θ_p zwischen optischer Achse und Pumpstrahl ändert (je größer θ_p , desto mehr überlappen die Kegel). Dabei kann man drei Situationen unterscheiden:

Zum einen, dass sich die zwei Kegel nicht schneiden. In diesem Fall sind die zwei Tochterphotonen stets durch ihre Polarisation unterscheidbar. Sie befinden sich immer in verschiedenen räumlichen Moden.

Dann gibt es einen Winkel θ_p , bei dem sich die Kegel gerade berühren. Das Licht, das entlang der Berührungsgereaden läuft, ist gänzlich unpolarisiert. Beide Photonen befinden sich in der gleichen räumlichen Mode ("kollinear" Fall).

Und schließlich schneiden sich die zwei Kegel ab einem bestimmten Wert von θ_p . Sammelt man das Licht entlang der zwei Schnittgeraden – den räumlichen Moden 1 und 2 – auf, so ist es in jeder einzelnen Mode wiederum unpolarisiert. Man kann nicht unterscheiden, ob das aufgesammelte Photon vom ordentlich polarisierten oder vom außerordentlich polarisierten Kegel stammt. Stellt es sich jedoch nach Messung als ordentlich polarisiert heraus, kann man mit Sicherheit vorhersagen, dass das Schwesterphoton in der anderen Mode außerordentlich polarisiert detektiert wird – und umgekehrt.

Man beobachtet also einen verschränkten Zweiteilchenzustand, der sich als

$$|\Psi\rangle = (|HV\rangle + e^{i\varphi}|VH\rangle) / \sqrt{2} \quad (4.3)$$

schreiben lässt [34]. Die relative Phase φ rührt von den unterschiedlichen optischen Weglängen für horizontale beziehungsweise vertikale Polarisation im doppelbrechenden Kristall her. Sie kann leicht kompensiert werden (vgl. Kap. 4.2.3).

4.2.3 Die Photonenpaarquelle

Der nichtlineare Kristall

Abbildung 4.2 stellt den Aufbau der Quelle schematisch dar. In unserem Fall kommt als nichtlineares Medium ein 2 mm langer Kristall aus β -Barium Borat (β -BaB₂O₄, BBO) zum Einsatz.

Seine Oberflächen sind bei den Wellenlängen des Pumpasers und der SPF-Photonen, also bei 351 nm und 702 nm, anti-reflex beschichtet.

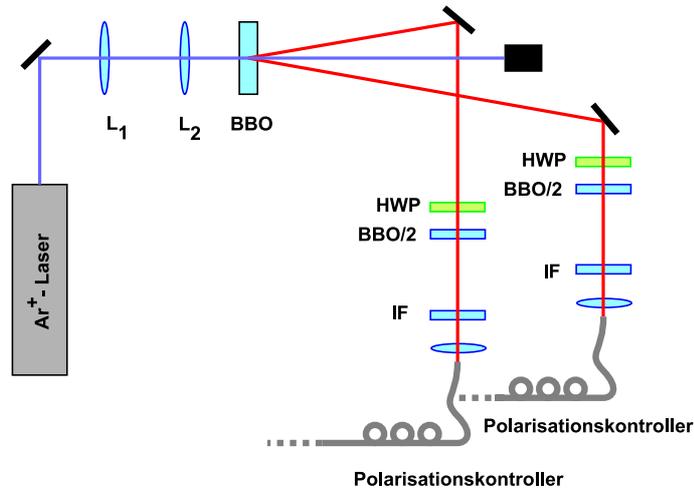


Abbildung 4.2: Der kompakte Quellenaufbau zur spontanen parametrischen Fluoreszenz. Die Abmessungen sind etwa $30\text{ cm} \times 30\text{ cm}$. Die Linsen L_1 und L_2 präparieren die gewünschte Strahltaile am nichtlinearen Kristall BBO. Die Halbwellenplättchen HWP auf 45° drehen die Polarisation, bevor die Kompensatorkristalle BBO/2 durchlaufen werden. Mit IF sind zwei Interferenzfilter bezeichnet. Danach wird in single-mode Fasern eingekoppelt.

Da wir vollkommen ununterscheidbare Photonen benötigen, müssen wir $\lambda_1 = \lambda_2 = 2\lambda_p = 702\text{ nm}$ präparieren. Das entspricht dem entarteten Fall der SPF. Der Kristall wurde also so geschnitten, dass bei senkrechtem Einfall des Pumpstrahls $\theta_p = 49.7^\circ$ ist. Dann nämlich schneiden sich die zwei Kegeloberflächen senkrecht, und die spektrale Verteilung ist in beiden Moden symmetrisch um die Aufsammlpunkte.

Da wir aus einem endlichen, rotationssymmetrischen Raumwinkel Photonen aufsammeln, ist in dieser Konfiguration die Kopplungseffizienz in single-mode Fasern am größten.

Der Winkel zwischen den zwei Moden, die symmetrisch um den Pumpstrahl angeordnet sind, beträgt ungefähr 6° [33, 35]. Unter diesem Winkel stehen zwei Spiegel hinter dem BBO-Kristall und lenken das Licht der SPF zu den Einkopplfasern um. Dieser gefaltete Strahlengang macht den Aufbau sehr kompakt.

Walk-Off Kompensation

Die Doppelbrechung im BBO-Kristall bewirkt unterschiedliche Brechungsindizes und damit unterschiedliche Emissionsrichtungen der ordentlich bzw. außerordentlich polarisierten SPF-Photonen. Dadurch wird die Mode ordentlicher Polarisation räumlich aufgeweitet und die Mode außerordentlicher Polarisation relativ zur Pumpstrahlrichtung vor dem Kristall versetzt (transversaler Walk-Off). Die räumlichen Moden liegen damit

nicht mehr exakt übereinander und mindern den Grad der Verschränkung⁴.

Des Weiteren werden die zwei Polarisationskomponenten zeitlich separiert (longitudinaler Walk-Off). Dieser Zeitunterschied liegt für die verwendete Kristalllänge (2 mm) und die Doppelbrechung $\Delta n := n_e - n_o = -0.11$ in der Größenordnung der Kohärenzlänge der Einzelphotonen und muss daher kompensiert werden, um auszuschließen, dass die unterschiedlich polarisierten Photonen aufgrund ihrer Ankunftszeit unterschieden werden können.

Um die Auswirkungen dieser zwei unerwünschten Effekte auf die Verschränkung zu reduzieren, stellt man in die Strahlengänge der beiden Moden je ein Halbwellenplättchen auf 45° (entspricht σ_x aus Gl. 2.22), das horizontale auf vertikale Polarisation vertauscht. Danach durchlaufen die Photonen je einen BBO-Kristall mit der halben Dicke des SPF-Kristalls, in denen sich die Walk-Offs wegen der vertauschten Polarisation teilweise kompensieren [33].

Es zeigt sich, dass durch diese Anordnung zwar nicht die Aufweitung der anfangs ordentlichen Mode, wohl aber der Versatz der außerordentlichen Mode kompensiert werden kann, sodass sie beide symmetrisch um die gleiche Achse propagieren. Der longitudinale Walk-Off kann im Mittel (die Entstehungsorte der Paare variieren wegen der großen Kohärenzlänge des Lasers über die gesamte Länge des Kristalls) ebenfalls kompensiert werden.

Durch einfaches Verkippen eines Kompensator-Kristalls in einem Arm kann man einen relativen Phasenschub zwischen der horizontalen und vertikalen Polarisationskomponente auf das entsprechende Teilchen (lokale unitäre Operation) erreichen und somit die relative Phase φ in Gl. 4.3 einstellen.

Ganz offensichtlich machen wir hier wieder von der Tatsache Gebrauch, dass die maximal verschränkten Zustände (2.59) durch lokale unitäre Transformationen ineinander überführbar sind. Im Speziellen können wir an dieser Stelle zwischen $|\Psi^-\rangle$ und $|\Psi^+\rangle$ (entsprechend $\varphi = \pi$ bzw. $\varphi = 0$ in Gl. 4.3) wählen.

Pumplaser und Einkopplung

Der BBO-Kristall wird von einem Ar^+ -Laser⁵ gepumpt. Er liefert UV-Licht bei $\lambda_p = 351.1$ nm mit einer Kohärenzzeit von etwa 17 ns $\approx 5\text{m}/c$ [36] bei einer Ausgangsleistung von etwa 75 mW bis 150 mW am Kristall. Ein Etalon im Laserresonator sorgt dafür, dass nur eine longitudinale Mode resonant ist.

Das emittierte Strahlprofil ist das der TEM_{00} Mode, also einer Gaußschen Mode. Direkt

⁴Die Polarisation der Photonen könnte aus ihrer Position geschlossen werden.

⁵”Spectra Physics BeamLok”

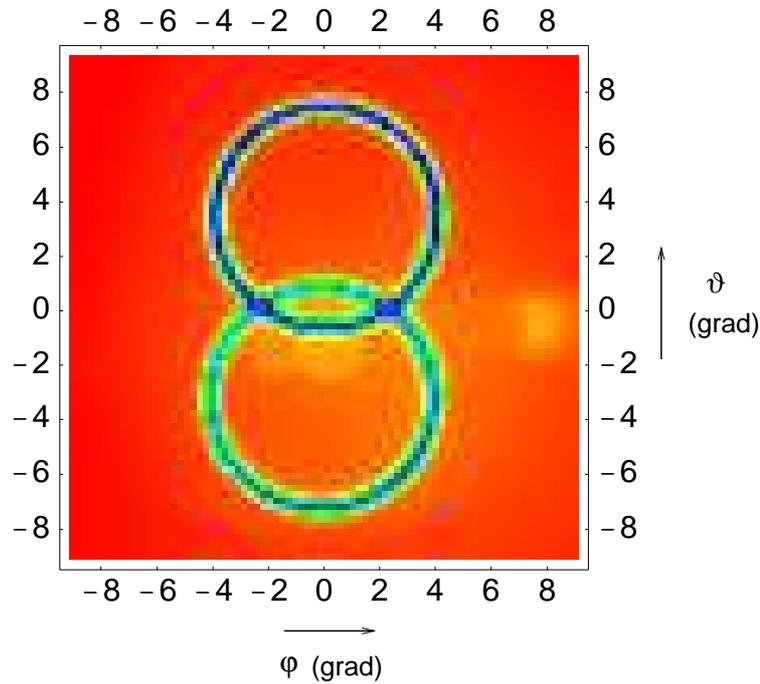


Abbildung 4.3: Abhängigkeit der Fluoreszenzintensität bei 702 nm (Bandbreite 5.5 nm) vom horizontalen und vertikalen Emissionswinkel [33].

hinter dem Laser werden über ein Prisma unerwünschte Teile des Spektrums, die durch Fluoreszenz im Gasmedium entstehen, aus dem Strahl separiert. Danach sorgen zwei Linsen dafür, dass die Taille des Gaußschen Pumpstrahls genau im BBO-Kristall liegt und dort eine Größe w_0^p hat.

Jeder Gaußsche Strahl wird durch seine Wellenlänge und Ort bzw. Größe der Taille w_0 (engl. "waist") eines Gaußschen Strahls definiert. Die radiale Intensität einer Gaußschen Mode ist proportional zu $\exp(-2r^2/w_0^2)$, wobei r der radiale Abstand vom Strahlmittelpunkt $r = 0$ ist, wo die Intensität maximal ist; bei $r = w_0$ ist die Intensität also auf $1/e^2$ abgefallen. Ein Gaußscher Strahl weitet sich weit weg von der Strahltaile, also in einer Entfernung, die groß gegen die Rayleighlänge⁶ $z_R = \frac{w_0^2 \pi}{\lambda}$ ist, mit einem Winkel $\theta_{\text{div}} = \frac{w_0}{z_R}$ gegen die Ausbreitungsrichtung auf.

Um das Fluoreszenzlicht von möglichst wohldefinierten räumlichen Moden um die Schnittgeraden aus Abb. 4.1 aufzusammeln, koppeln wir das Licht in single-mode Glasfasern. In diese kann man die Gaußsche TEM_{00} - Mode des elektrischen Feldes einkoppeln, wenn die Wellenlänge des zu führenden Lichts größer als die Grenzwellenlänge⁷ ist.

⁶Im (longitudinalen) Abstand z_R von der Taille hat der Strahl die doppelte Fläche.

⁷Im Fall der hier verwendeten Faser P1-3224-FC der Firma Thorlabs 630 nm

Dieses Aufsammeln in die Glasfasern konnte effizient durch ein in [35] vorgestelltes Verfahren durchgeführt werden, das ich hier kurz skizzieren möchte.

Wir beginnen damit, dass wir eine bestimmte spektrale Bandbreite $\Delta\lambda$ der aufgesammelten Photonen in der TEM_{00} - Mode der Faser vorgeben. Da die Wellenlänge der emittierten Photonen entlang der Aufsammelgeraden (wo $\lambda = 2\lambda_p$ ist) vom Emissionswinkel θ abhängt, entspricht der gewünschten spektralen Bandbreite $\Delta\lambda$ des aufgesammelten Lichts ein Winkelbereich $\Delta\theta = \frac{d\theta}{d\lambda}\Delta\lambda$ der Emission [35] (vgl. Abb 4.3). Dieser – als Divergenzwinkel θ_{div} einer Gaußschen Mode interpretiert – definiert zusammen mit der Zentralwellenlänge $\lambda = 702$ nm den Parameter w_0 der Gaußschen Mode.

Diese Fluoreszenzmode soll ihren Ursprung im Zentrum des BBO-Kristalls haben. Es werden also nur Fluoreszenzphotonen aufgesammelt, die in dem Bereich des Kristalls entstehen, der mit der eben berechneten Mode überlappt.

Die Ausbeute an Photonen, die in diesem Bereich entstehen, ist maximal, wenn dieser Bereich mit der Pumpstrahlmode zusammenfällt. Dann ist es am besten, wenn die Strahltaile des Pumpstrahls ebenfalls auf diese Region fokussiert wird: $w_0 = w_0^p$.

Somit können wir aus einer gewünschten Breite $\Delta\lambda$ die für effiziente Kopplung benötigte Pumpstrahltaile w_0^p berechnen. Die Fluoreszenzmoden (Ort und Größe der Taile bekannt) können dann mit je einer Linse, deren Brennweite vom Abstand zwischen Faserende und Kristall abhängt, auf die Öffnung der single-mode Faser abgebildet werden. Die Quelle wurde auf ein Fluoreszenzspektrum von $\Delta\lambda = 4$ nm Halbwertsbreite ausgelegt. Daraus ergibt sich der Divergenzwinkel der Fluoreszenzmode $\theta_{\text{div}} = 0.186^\circ$ und für die Linsen mit Brennweite von 11 mm eine Entfernung von 34.1 cm zwischen Faser und Kristall [36] (Das Faserende steht im Brennpunkt der Linse).

Die Strahltaillen der SPF-Moden sind $w_0 = 68.5\mu\text{m} = w_0^p$.

Um zu verhindern, dass vom Pumpstrahl UV-Licht mit aufgesammelt wird, stehen vor den Faserkopplern Interferenzfilter mit einer Halbwertsbreite von 5 nm um 702 nm. Diese Filter erleichtern auch erheblich die Justage der Quelle, da man mit ihnen nur Photonen mit etwa der richtigen Wellenlänge $2\lambda_p$ aufammelt.

Die Photonen der SPF laufen über die zwei Glasfasern, in die wir durch diesen Prozess eingekoppelt haben, zu zwei anderen Faserkopplern, wo das Licht in die zwei Arme 1 und 2 wieder ausgekoppelt wird.

4.3 Zur Detektion der Einzelphotonen

Da die Photonenpaare der SPF gleichzeitig entstehen, können sie in Koinzidenz gemessen werden. Da während einer kurzen Zeitspanne (ungefähr 10 ns) nur mit geringer Wahrscheinlichkeit ein SPF-Paar erzeugt wird⁸, können zwei Photonen, die innerhalb ei-

⁸Die Rate der detektierten Paare ist maximal in der Größenordnung 10^5 pro Sekunde.

nes kleinen Koinzidenzzeitfensters τ_C detektiert werden, dem selben Fluoreszenzprozess zugeordnet werden. Nur von diesen können wir die gewünschte Verschränkung erwarten.

Durch Verluste (zum Beispiel durch Reflexionen an optischen Elementen, Absorption in den Fasern, Streuung etc.) und die nicht optimale Effizienz der Detektoren (Quanteneffizienz etwa 40%) werden nicht alle erzeugten Paare als Koinzidenzen detektiert. Deswegen sind die Einzelzählraten in den zwei Armen stets größer als die Koinzidenzrate zwischen ihnen.

Typische Werte sind $\leq 10^5$ Einzelereignisse ("Singles") pro Sekunde, und das Verhältnis Einzel- zu Koinzidenzzählrate war maximal 24% (ohne Interferenzfilter bei der Quelle). Unkorrelierte Einzelereignisse produzieren zufällige (also "unechte") Koinzidenzereignisse mit einer Rate $R_a = \tau_C \cdot R_1 R_2$, wenn $R_{1/2}$ die Einzelzählraten sind. Diese Koinzidenzen rühren von dem endlichen Koinzidenzzeitfenster her, sind rein statistischer Natur, und können deswegen von der gemessenen Koinzidenzrate abgezogen werden.

Die Einzelphotonendetektion geschieht mit Silizium Avalanche Photodioden, die im Geigermodus betrieben werden. Ein einfallendes Photon erzeugt im aktiven Volumen des Halbleiters ein Elektron-Loch Paar⁹. Durch eine angelegte Hochspannung in Sperrrichtung werden diese Ladungsträger so stark beschleunigt, dass sie eine ganze "Lawine" von Ladungsträgern erzeugen, was zu einem Spannungspuls am Messwiderstand führt.

Danach geht die Diode nach einer Totzeit von etwa $1 \mu s$ wieder in ihren ursprünglichen Zustand über. Sie sättigt erst bei Zählraten jenseits von circa 10^5 Hz.

Der auf diese Weise vom Photon erzeugte elektrische Puls wird dann mithilfe einer Schwellenwertlogik in ein digitales Signal umgesetzt und in digitaler Schalttechnik prozessiert. Es kann so von einem Computer erfasst werden.

Wegen der beschriebenen Arbeitsweise im Geiger-Modus ist die Photodiode unempfindlich gegenüber der Photonenzahl. Das heißt, dass man nicht unterscheiden kann, ob ein oder mehrere Photonen einen gemessenen Puls ausgelöst haben.

Man kann jedoch mit einer gewissen Wahrscheinlichkeit unter Verwendung von Strahlteilern und Photodioden trotzdem nachweisen, dass (mindestens) zwei Photonen in einer Mode waren. Laufen zum Beispiel zwei Photonen in der selben Mode, teilen sie sich in der Hälfte der Fälle an einem 50-50 Strahlteiler auf und können dann in zwei verschiedenen Moden nachgewiesen werden.

In der anderen Hälfte der Fälle nehmen beide Photonen den selben Strahlteiler ausgang und lösen ein einziges Signal an einem Detektor aus.

Wenn man die Fälle selektiert, in denen man eine Koinzidenz an zwei Detektoren zwischen den beiden Strahlteilermoden gesehen hat, kann man also auch zwei Photonen in einer Mode – der *vor* dem Strahlteiler – nachweisen¹⁰. Ich werde an gegebener Stelle im

⁹Das Material ist bei der verwendeten Wellenlänge (702 nm) besonders empfindlich.

¹⁰Die stark unterdrückten SPF-Prozesse mit mehr als zwei Photonen können in diesem Experiment

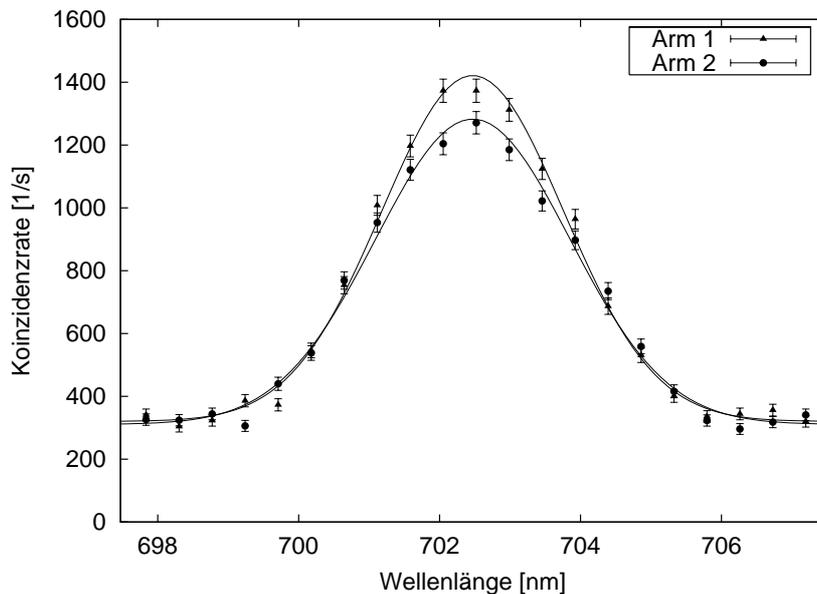


Abbildung 4.4: Die Spektren der Einzelphoton-Ereignisse aus Arm 1 und 2. Messzeit pro Punkt 1 Sekunde.

Experiment darauf hinweisen, wenn wir hiervon Gebrauch machen.

4.4 Die Spektren der Einzelphotonen

Zum Einstellen und Überprüfen der Einzelphotonenspektren wurde jeweils ein Photon als zeitliche Referenz detektiert, das andere durch ein Spektrometer geschickt und dann in Koinzidenz detektiert. Das Einzelphotonen-Spektrometer besteht aus einem drehbaren Gitter, an dem das einfallende Licht gebeugt wird. Die erste Beugungsordnung wird über einen Spiegel und eine Linse in eine multi-mode Faser eingekoppelt.

Durch Justage der Faserkoppler an der Quelle und an den entsprechenden Spiegeln (siehe Abb. 4.2) können die Spektren der aufgesammelten Fluoreszenzmoden variiert werden. Abb. 4.4 und 4.5 zeigen das Ergebnis eines solchen Justagevorgangs. Man sieht, dass die Spektren der Photonen in den zwei Armen sowohl bei Einzel- als auch Koinzidenzereignissen sehr gut übereinstimmen. Die Zählraten der Koinzidenzen sind sensibel auf Verluste in *beiden* Armen und deswegen deutlich geringer. Der konstante Offset bei den Einzelereignissen kommt von der Dunkelzählrate¹¹ des Detektors. Bei den niedrigen Einzelzählraten ($< 10^4$ pro s) können zufällige Koinzidenzen vernachlässigt werden.

vernachlässigt werden.

¹¹Konstanter Untergrund an Zählrate; wird durch thermische Erzeugung von Elektron-Loch Paaren im Detektorhalbleiter hervorgerufen

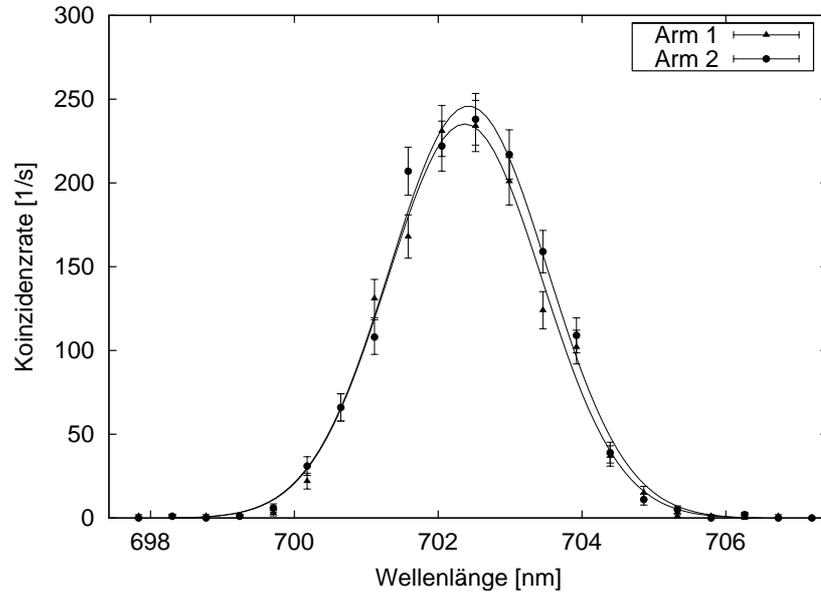


Abbildung 4.5: Die Spektren der in Koinzidenz gemessenen Photonen aus Arm 1 und 2. Messzeit pro Punkt 1 Sekunde

Für die Einzelphotonen (Abb. 4.4) ergibt die Messung eine Halbwertsbreite von 3.05 nm (3.25 nm) um $\lambda_{S,1/2} = 702.47$ nm (in beiden Armen innerhalb des Fehlerbereichs von ± 0.05 nm gleich) in Arm 1 (2), bei den Koinzidenzen (Abb. 4.5) erhalten wir¹² FWHM=2.53 nm (2.58 nm) bei $\lambda_{K,1} = 702.37$ nm ($\lambda_{K,2} = 702.42$ nm) für Arm 1 (2). Die Differenz zwischen den Zentralwellenlängen für Koinzidenzen liegt damit unter 2% der spektralen Breite (FWHM).

Die Breite der Spektren hängt empfindlich von der Entfernung der Linsen L_1 und L_2 ab. Sie wird durch die Interferenzfilter etwas verringert. Man sieht, dass die spektralen Breiten etwas geringer sind, als beim Quelledesign beabsichtigt (4 nm). Die Einkopplung in die Quellenfasern könnte also noch dahingehend optimiert werden, dass ein größerer Wellenlängenbereich (Winkelbereich der Fluoreszenz) aufgesammelt wird, wodurch auch insgesamt mehr SPF-Koinzidenzen aufgesammelt würden.

Die Tatsache, dass die Wellenlängen $\lambda_{K,1}, \lambda_{K,2}$ nicht exakt gleich der doppelten Wellenlänge der Pump photons (702.2 nm) entspricht, rührt wohl von einer leichten Dejustierung des Spektrometers her. Jedenfalls weiß ich nicht, wo die Wellenlänge der Photonen sich hätte ändern können. Für unsere Belange wichtig ist daneben nur, dass Wellenlängen möglichst gleich justiert wurde. Das konnte verifiziert werden.

Dies wird notwendig in Kap. 5.5.1, wo wir uns das Phänomen der Interferenz der Photonen zunutze machen. Dazu müssen die Photonen – eben auch in der Frequenz bzw. Wellenlänge – ununterscheidbar sein.

¹²FWHM engl. "full width at half maximum": Halbwertsbreite einer gaußförmigen Verteilung.

4.5 Die Polarisationsverschränkung

4.5.1 Transformation des Quellenzustands

Die Photonen laufen auf dem Weg von der SPF-Quelle zum Messaufbau durch Glasfasern, die durch Spannung (Krümmung der Faser) induzierte Doppelbrechung aufweisen und somit die Polarisation des in der Faser propagierenden Lichts drehen. Dies stellt eine (unbekannte) unitäre Transformation der Photonenpolarisation dar. Solche Transformationen haben wir bereits in Kap. 2.2.4 theoretisch untersucht und gelernt, dass sie den Verschränkungsgrad nicht beeinflussen. Damit können wir die inverse Operation auf jedes¹³ Photon anwenden und somit den ursprünglichen (oder einen anderen, maximal verschränkten) Zustand erzeugen.

Zu diesem Zweck wurde jede einzelne der zwei Fasern durch so genannte Polarisationskontrollen geführt. In einem solchen kann die Polarisation beliebig gedreht werden, indem Doppelbrechung durch Faserkrümmung erzeugt wird. Eine Faser kann also im obigen Sinn "neutral" gemacht werden, indem vor den Faserkoppler am Eingang der Faser (bei der Quelle) ein Polarisator auf 0° – entsprechend horizontaler Polarisation – in den Strahlengang gestellt wird und hinter den Faserkoppler am Ende der Faser ein zweiter Polarisator auf 90° (linear vertikale Polarisation). Dann wird der Polarisationskontrollen so eingestellt, dass möglichst kein Licht mehr hinter dem zweiten Polarisator ankommt.

Das wird für die andere Faser ebenfalls durchgeführt. Davor müssen die Fasern fest fixiert werden, um auszuschließen, dass sie sich – einmal neutral gemacht – nochmal bewegen und somit eine andere Drehung der Polarisation verursachen.

Durch das beschriebene Verfahren wird sichergestellt, dass die Doppelbrechung der Faser nicht horizontale in vertikale lineare Polarisation dreht. Ein Phasenschub zwischen H und V ist immer noch möglich¹⁴. Dieser kann jedoch an einem der Kompensationskristalle justiert werden, wie in Kap. 4.2.3 dargelegt. Der Zustand *hinter* den Fasern hat also mit "neutralen" Fasern wieder die gleiche Form $|\Psi\rangle = (|HV\rangle + e^{i\varphi}|VH\rangle)/\sqrt{2}$ wie davor (mit anderem φ , siehe Gl. 4.3). Insbesondere können wir mit einem Kompensatorkristall $e^{i\varphi} = i$ einstellen. Diesen Zustand, $|\Psi_i\rangle := (|HV\rangle + i|VH\rangle)/\sqrt{2}$, können wir dann wie folgt *lokal* in die vier Bell-Zustände transformieren:

Das Photon in Arm 1 (vgl. Abb. 4.6) durchläuft zunächst ein Halbwellenplättchen (HWP), das auf den Winkel¹⁵ α eingestellt ist, und dann ein Viertelwellenplättchen (QWP) auf Winkel β . Durch vier bestimmte Kombinationen (α, β) können somit aus

¹³In der Tat erfahren beide Photonen eine unitäre Transformation; diese sind jedoch lokal, also als Produkt $U_1 \otimes U_2$ darstellbar und somit auch lokal umkehrbar.

¹⁴Um diesen ebenfalls zu eliminieren müsste die selbe Prozedur noch mit unter $+45^\circ / -45^\circ$ (P/M) eingestellten Polarisatoren durchgeführt werden.

¹⁵Definitionen der Operatormatrizen und Winkel für Wellenplättchen in A.2.

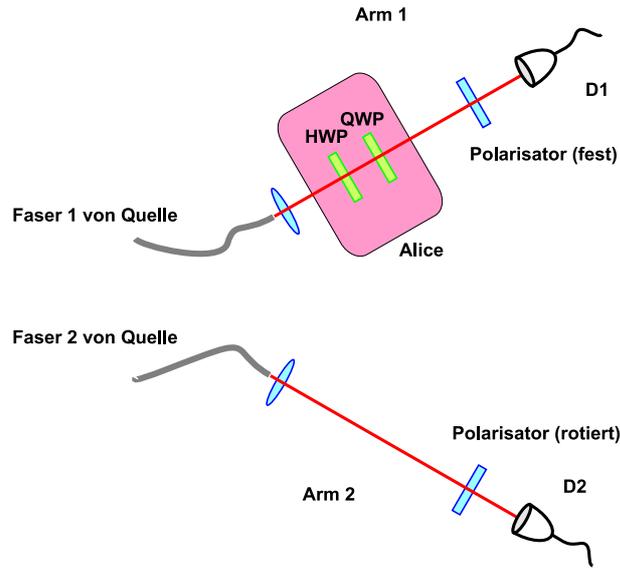


Abbildung 4.6: Schema des Aufbaus zur Messung der Polarisationskorrelationen. Im farblich hinterlegten Bereich findet Alices Informationskodierung statt.

dem Zustand $|\Psi_i\rangle$ alle vier Bell-Zustände generiert werden:

$$U_{\lambda/4}(\beta) U_{\lambda/2}(\alpha) |\Psi_i\rangle = \begin{cases} |\Psi^-\rangle & \text{für } \alpha = 0^\circ \text{ und } \beta = 0^\circ \\ |\Psi^+\rangle & \text{für } \alpha = 0^\circ \text{ und } \beta = 90^\circ \\ |\Phi^-\rangle & \text{für } \alpha = 45^\circ \text{ und } \beta = 0^\circ \\ |\Phi^+\rangle & \text{für } \alpha = 45^\circ \text{ und } \beta = 90^\circ \end{cases} \quad (4.4)$$

Man beachte, dass diese Operatoren genau den vier unitären Operatoren U_{00}, U_{01}, U_{10} und U_{11} entsprechen, die Alice im Dense-Coding-Protokoll durchzuführen hat. Sie erzeugt aus einem Anfangszustand durch eine von vier Operationen an nur ihrem Teilchen – entsprechend einer der vier Winkelkombinationen aus Gl. 4.4 – *lokal* alle vier Bell-Zustände. Bobs Teilchen in Arm 2 bleibt unangetastet.

Wir sehen also, dass genau hier Alices klassische Information durch ihre Wahl der Position der Wellenplättchen in das System kodiert werden kann.

Im folgenden Abschnitt zeige ich, dass dadurch wirklich die vier Bell-Zustände erzeugt werden.

4.5.2 Die Polarisationskorrelationen

Die Bell-Zustände zeigen nichtklassische Korrelationen in beliebigen Basen. Zum Nachweis, dass ich mit dem hier beschriebenen Prozess der spontanen parametrischen Fluoreszenz vom Typ II, der Methode zur Kopplung in die Glasfasern, und der unitären

Operationen vom vorigen Abschnitt tatsächlich diese vier Zustände generieren kann, analysieren wir die Polarisationskorrelationen der zwei Photonen zuerst in der Standardbasis $\{|H\rangle, |V\rangle\}$ und dann in der konjugierten Basis $\{|P\rangle, |M\rangle\}$.

Abbildung 4.6 zeigt schematisch den Aufbau zur Messung der Polarisationskorrelationen. In Arm 1 steht ein Polarisator auf H (beziehungsweise P), während in Arm 2 ein Polarisator von 0° bis 360° von einem Motor durchgedreht wird. Dies geschieht in Schritten von 5° und in jeder Position werden die Koinzidenzereignisse zwischen den Detektoren 1 und 2 genau 1 Sekunde lang gezählt.

Die Photonen werden in multi-mode Fasern eingekoppelt, die einen wesentlich größeren Akzeptanzraumwinkel als single-mode Fasern aufweisen. Damit ist man nicht so sensibel auf einen etwaigen Strahlversatz durch den sich drehenden Polarisator¹⁶.

Aus den Gleichungen 2.50-2.53 und 2.57 kann man die Art der erwarteten Korrelationen in den Basen H/V und P/M für alle vier Zustände ablesen.

In den Abb. 4.7 sind die Ergebnisse dieser Messungen gezeigt. Sie zeigen die erwarteten Korrelationen für alle (gemäß Gl. 4.4) eingestellten Bell-Zustände. Dabei ist die Koinzidenzrate aufgetragen, die man an den Detektoren erhält, wenn das Photon in Arm 1 horizontal (H) bzw. unter $+45^\circ$ (P) polarisiert war. Die Winkel entsprechen bei 0° (90°) dem Polarisationszustand $|H\rangle$ ($|V\rangle$), bei 45° ($-45^\circ = 135^\circ$) dem Polarisationszustand $|P\rangle$ ($|M\rangle$).

Zum Beispiel gilt für den EPR-Zustand $|\Psi^-\rangle$: Bei parallelen Polarisatoren (HH bzw. PP) sind die Koinzidenzen minimal, bei gekreuzten (HV bzw. PM) dagegen maximal. Daran können wir erwartungsgemäß ablesen, dass der Zustand in beiden Basen antikorreliert ist. Für diesen Zustand und bei gekreuzter Einstellung in PM-Basis wurde die Verkipfung des Kompensationskristalls (Kap. 4.2.3) eingestellt, indem auf minimale Koinzidenzen justiert wurde. Der Kontrast¹⁷ der Korrelationen ist in Tabelle 4.1 angegeben.

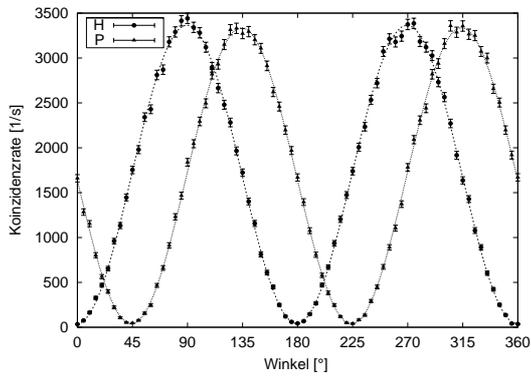
Basis	$ \Psi^-\rangle$	$ \Psi^+\rangle$	$ \Phi^-\rangle$	$ \Phi^+\rangle$
H/V	98.2	98.0	98.0	98.1
P/M	98.4	98.8	98.9	98.3

Tabelle 4.1: Gemessene Kontraste der Polarisationskorrelationen in Prozent für die Bell-Zustände in H/V-Basis beziehungsweise P/M-Basis.

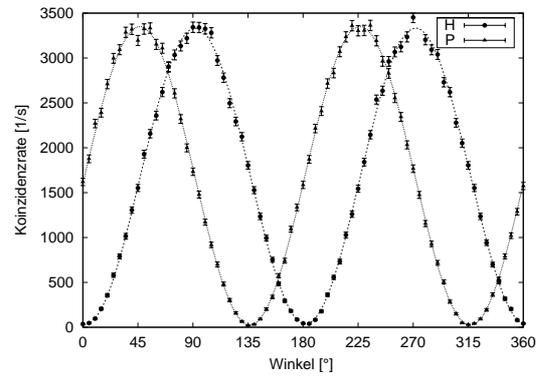
Da die hohen Einzelzählraten bei dieser Messung einen Untergrund von ungefähr 10 zufälligen Koinzidenzen pro Sekunde von unkorrelierten Photonen verursachen, wurde

¹⁶Genauer dazu in Kap. 5.5.2.

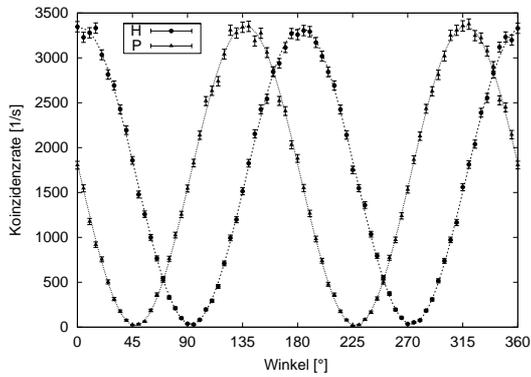
¹⁷Zur Definition des Begriffs siehe Anhang A.1.



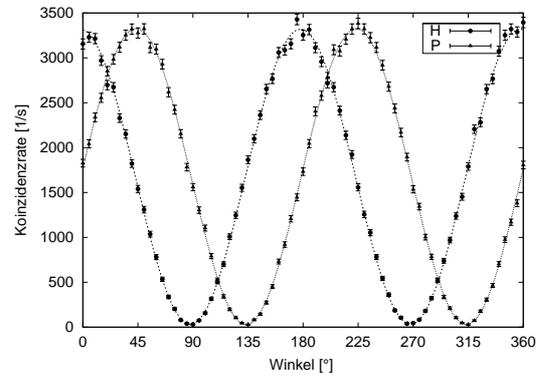
(a) Zustand $|\Psi^-\rangle$ eingestellt



(b) Zustand $|\Psi^+\rangle$ eingestellt



(c) Zustand $|\Phi^-\rangle$ eingestellt



(d) Zustand $|\Phi^+\rangle$ eingestellt

Abbildung 4.7: Verlauf der Polarisation des einen Photons, wenn das andere Photon horizontal (H) bzw. unter $+45^\circ$ (P) polarisiert detektiert wird. Die Balken geben die statistischen Fehler an; zufällige Koinzidenzen wurden subtrahiert.

dieser Wert von den gemessenen Raten abgezogen, um ein genaueres Maß (den Kontrast) für die tatsächliche Verschränkung der korrelierten Paare zu erhalten. Die unkorrigierten Kontraste sind etwa 0.5% geringer.

Die Werte wurden durch einen "fit" der sinusförmigen Funktion¹⁸ f_{sin} an die Messpunkte für jeden einzelnen Bell-Zustand und jede Basis ermittelt. Dabei wurden die Messwerte gemäß ihres statistischen Fehlers gewichtet. Der absolute Fehler der Angaben

¹⁸siehe Anhang A.1.

liegt bei $\pm 0.2\%$. Damit konnte gezeigt werden, dass alle vier polarisationsverschränkten Bell-Zustände mit sehr hohem Kontrast erzeugt werden können. Durch die in Gl. 4.4 beschriebenen Operationen können wir *lokal* aus einem Anfangszustand alle Bell-zustände erzeugen. Wie in Kap. 3 dargelegt, ist dies der wesentliche Schritt im *dense coding*-Protokoll.

5 Vollständige Bell-Zustandsanalyse

Inhalt

5.1	Einleitung	58
5.2	Unterscheidbarkeit der Bell-Zustände	59
5.3	Das CNOT Gatter	61
5.3.1	Vollständige Gattersysteme	61
5.3.2	Das CNOT als maximal verschränkendes Gatter	62
5.4	Verschränkung in mehreren Freiheitsgraden	63
5.5	Implementierung	65
5.5.1	HOM-Interferenz	67
5.5.2	Das asymmetrische Interferometer	71
5.5.3	Analyse in P/M-Basis	73
5.5.4	Die Detektoreinheit	76
5.5.5	Die Koinzidenzeinheit	80
5.6	Ergebnisse	83

5.1 Einleitung

Die Bell-Zustände spielen in der Quanteninformationstheorie eine herausragende Rolle. Sie bilden eine *maximal* verschränkte Basis im Zwei-Qubit Hilbertraum, sind also paarweise orthogonal und damit durch eine geeignete Messung absolut unterscheidbar. Projiziert man einen Produktzustand auf die Bell-Basis, so befindet sich das System nach der Messung in einem der Bell-Zustände (vgl. Kap. 2.2.3).

Diese Eigenschaft macht man sich unter anderem beim Teleportieren [37] zunutze, wo man durch Projektion eines Zweiteilchenzustandes (A und B) auf die Bell-Basis den Quantenzustand eines dieser zwei Teilchen (B) über beliebige Distanzen auf ein drittes (C) übertragen kann. Teilchen A und C befanden sich zuvor in einem Bell-Zustand.

Nach der Projektion findet man natürlich A und B in einem der maximal verschränkten Basiszustände.

Die Projektion auf die Bell-Zustände ist ebenfalls der wesentliche Bestandteil der Verschränkungsübertragung [2, 38, 39] (engl. "entanglement swapping"), die es erlaubt, zwei weit entfernte Teilchen zu verschränken, ohne eine gemeinsame Messung an beiden vorzunehmen; die zwei Teilchen müssen zuvor jeweils mit einem anderen verschränkt gewesen sein, an welchen dann die Projektion vorgenommen werden kann.

Durch eine Reihe solcher Übertragungen an vielen distanten Systemen könnte man sehr weit entfernte Systeme miteinander verschränken, auch wenn der Quantenkanal zwischen ihnen imperfekt ist [40], also Verluste und Dekohärenz aufweist. Diese zwei verschränkten Systeme könnte man zum Beispiel zur sicheren Kommunikation über quantalen Schlüsselaustausch über sehr große Distanzen verwenden [41].

Beim Dense Coding ist es – wie wir in Abschnitt 3 gesehen haben – erforderlich, einen Zustand herzustellen, aus dem Alice durch eine lokale Transformation, also durch Operation auf nur ihrem Teilchen, einen der vier Bell-Zustände generieren kann. Und zu guter letzt muss Bob in der Lage sein, die vier Bell-Zustände unterscheiden zu können. Er kann davon ausgehen, dass er *ausschließlich* einen dieser vier Zustände bekommt, also keine Superposition von ihnen¹ bekommt. Eine solcher Vorgang wird auch als Zustandsklassifizierung oder -diskriminierung bezeichnet. Die Präparation des Anfangszustands und Alices lokale Operationen wurden bereits im Kapitel 4 besprochen. Wenden wir uns nun also dem letzten Schritt, Bobs Zustandsanalyse, zu.

5.2 Unterscheidbarkeit der Bell-Zustände

Wie wir sehen werden, stellt die Unterscheidung der Bell-Zustände (wenn man nur ein einzelnes System von Quantenteilchen vorliegen hat) die größte experimentelle Herausforderung im Dense Coding-Protokoll dar. Obwohl die Bell-Zustände orthogonal und sie somit prinzipiell unterscheidbar sind – d.h., es gibt eine Messung, die sie unterscheidet –, gehören sie zu einer Klasse von Zuständen [42, 4], die mit *üblichen* und mit technisch vertretbarem Aufwand implementierbaren optischen Hilfsmitteln nicht absolut unterscheidbar sind. Genauer meint man damit passive linear-optische² Elemente, die sich aus Phasenschiebern und Strahlteilern bilden lassen [43]. Die Frage, warum man sich denn darauf beschränken sollte, wird hauptsächlich durch Gründe der Effizienz beantwortet. So ist der experimentelle Aufwand, bei Verwendung nichtlinearer Prozesse ungleich höher; außerdem muss man verstärkt mit unerwünschten Störungen am System,

¹Da die Bell-Zustände eine Basis in $\mathbb{H} \otimes \mathbb{H}$ bilden, kann jeder Zwei-Qubit Zustand als eine Superposition von ihnen angesehen werden.

²linear bedeutet in diesem Fall, dass die Erzeugeroperatoren der Ausgangsmoden Linearkombinationen der Erzeugeroperatoren der Eingangsmoden sind [4].

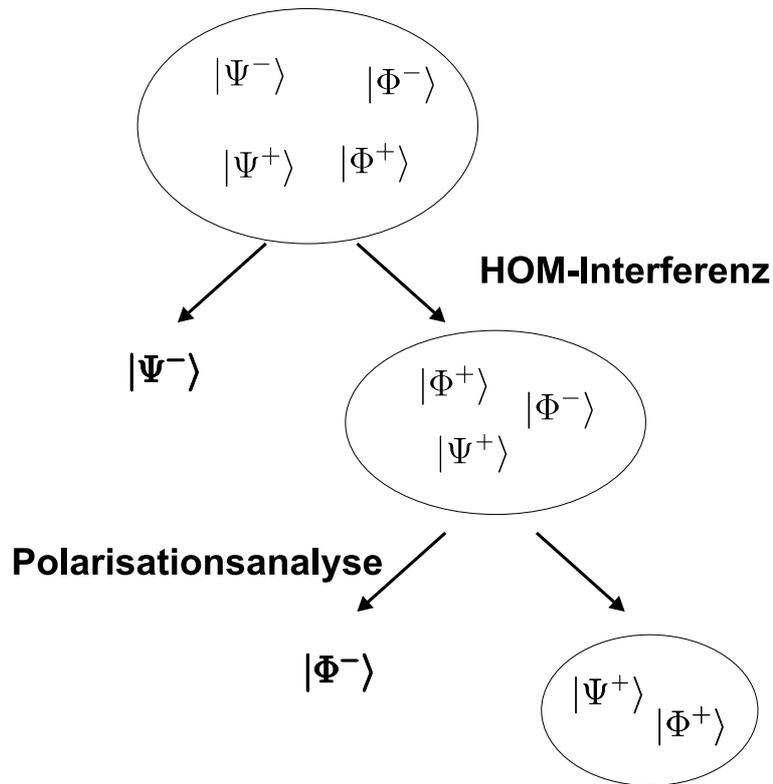


Abbildung 5.1: Mit passiven linearoptischen Elementen lassen sich deterministisch nur zwei Bell-Zustände unterscheiden. Das gilt für zwei beliebige Bell-Zustände. Hier sind es $|\Psi^-\rangle$ und $|\Phi^-\rangle$.

z.B. Dekohärenz, rechnen.

GHOSH ET AL. haben bewiesen [44], dass man bestenfalls zwischen zwei Bell-Zuständen unterscheiden kann, wenn man nur lineare Elemente und klassische Kommunikation verwendet; CALSAMIGLIA und LÜTKENHAUS verallgemeinern dieses Ergebnis und beweisen [4], dass die Erfolgswahrscheinlichkeit eines linearen Bell-Diskriminators nicht über 50% liegt³. Das schließt nichtdeterministische Analysen ein, bei denen jeder Zustand mit Wahrscheinlichkeit kleiner eins unterschieden wird.

Diese maximale Effizienz wurde in zahlreichen Experimenten, die auf ein- und zwei-Photoneninterferenz beruhen, erreicht [45, 46, 47].

Abb. 5.1 stellt die Stufen der Klassifizierung schematisch dar. Die HOM-Interferenz wird in Kap. 5.5.1 erklärt. Mit ihr lässt sich *ein* Zustand (z.B. $|\Psi^-\rangle$) unterscheiden. In einem weiteren Schritt kann ein anderer Zustand (z.B. $|\Phi^-\rangle$) diskriminiert werden, die

³Dabei nimmt man an, dass die Bell-Zustände gleichwahrscheinlich auftreten (die Entropie ihrer Verteilung also maximal ist).

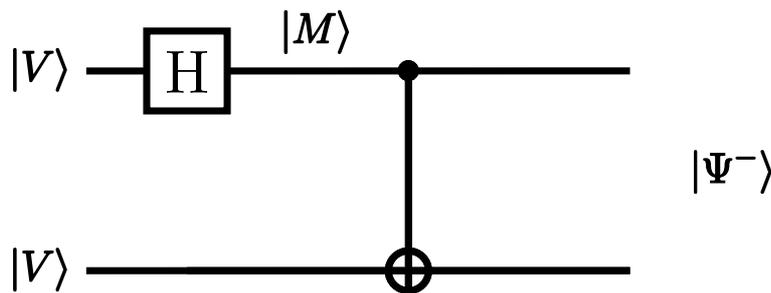


Abbildung 5.2: Das Ein-Qubit Hadamard Gatter bildet zusammen mit dem Zwei-Qubit CNOT-Gatter die Standardbasiszustände von $\mathbb{H} \otimes \mathbb{H}$ auf die Bellzustände ab und umgekehrt.

verbleibenden zwei (z.B. $|\Psi^+\rangle$, $|\Phi^+\rangle$) ergeben jedoch stets das gleiche – dritte – Resultat. Da jeder Bell-Zustand vor jedem Schritt durch eine unitäre Operation in einen anderen transformiert werden kann, kann man somit drei *beliebige* Klassen von Bell-Zuständen unterscheiden; nie jedoch alle vier gleichzeitig.

In der vorliegenden Arbeit demonstriere ich die experimentelle Umsetzung der *vollständigen* Bell-Zustandsanalyse. Das heißt, dass alle vier der Bell-Zustände deterministisch und an einer einzigen Kopie unterschieden werden können. Dabei verwenden wir nur passive linearoptische Elemente ohne bedingte Dynamik und ohne zusätzlicher Photonen. Wir nutzen die Verschränkung einzelner Photonenpaare in einem – neben der Polarisation – weiteren Freiheitsgrad aus, analysieren also in einem höherdimensionalen Hilbertraum (siehe Kap. 5.4).

5.3 Das CNOT Gatter

5.3.1 Vollständige Gattersysteme

Ein Computer ist eine sehr allgemeine, klassische Informationsverarbeitungsmaschine, die auf klassischer, Boolescher Logik basiert. In Analogie dazu kann man sich einen Quantencomputer vorstellen, der nun aber nach den Gesetzen der Quantenmechanik arbeitet. Natürlich tut das jeder klassische Computer in Strenge auch. Der Unterschied ist aber, dass der Quantencomputer vor allem die nichtklassischen Quanteneigenschaften seiner "Bauteile" nutzt, der herkömmliche Rechner jedoch nicht.

Eine klassische Rechenoperation kann durch (eventuell sehr viele) miteinander vernetzte Exemplare von sehr wenigen elementaren Gattern dargestellt werden. Tatsächlich reichen sehr wenige solcher Gatter aus (etwa das NOT und das XOR) um alle auf einem klassischen Computer durchführbaren Berechnungen zu implementieren.

Auch die Operationen eines allgemeinen Quantencomputers kann man als Netzwerk

elementarer Gatter darstellen. Diese stellen unitäre (reversible) Operationen auf einem oder mehreren Qubits dar. In diesem Fall können alle unitären Transformationen durch die Menge der unitären Ein-Qubit Operationen sowie einem verschränkenden Zwei-Qubit Gatter zusammengesetzt werden; ein solches ist das so genannte CNOT-Gatter.

Man kann es als quantale Verallgemeinerung des XOR Gatters verstehen⁴ mit dem entscheidenden Unterschied, dass es nicht nur für die Eingänge $|0\rangle$ und $|1\rangle$ (entsprechend 0 und 1 beim XOR) definiert ist, sondern eben auch für jede Superposition dieser (Basis-) Zustände, also jedes Qubit.

5.3.2 Das CNOT als maximal verschränkendes Gatter

Das CNOT-Gatter wirkt auf die Basiszustände folgendermaßen:

$$\begin{aligned}
 U_{\text{CNOT}} : \quad & |00\rangle \mapsto |00\rangle \\
 & |01\rangle \mapsto |01\rangle \\
 & |10\rangle \mapsto |11\rangle \\
 & |11\rangle \mapsto |10\rangle
 \end{aligned} \tag{5.1}$$

Das erste Qubit wird "control", das zweite "target" genannt. Das control-Qubit bestimmt, ob das target-Qubit verändert wird oder nicht. Es bleibt selbst unverändert. In einer physikalischen Realisierung müssten die zwei Qubits (control und target) sich also gegenseitig beeinflussen können.

Interessanterweise kann man den Prozess der Verschränkung, also die Transformation eines Produktzustandes in einen verschränkten Zustand, durch das CNOT-Gatter zusammen mit einem Hadamard-Gatter realisieren (Abb. 5.2).

Das Ein-Qubit Hadamard-Gatter transformiert die Ein-Qubit Basiszustände wie

$$H : \quad |0\rangle \mapsto (|0\rangle + |1\rangle)/\sqrt{2}, \quad |1\rangle \mapsto (|0\rangle - |1\rangle)/\sqrt{2} \tag{5.2}$$

Aus dem Produktzustand $|1\rangle|1\rangle \equiv |V\rangle|V\rangle$ wird also durch die Wirkung des Hadamard-Gatters auf das erste Qubit

$$|1\rangle|1\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle|1\rangle - |1\rangle|1\rangle), \tag{5.3}$$

was sich durch das CNOT-Gatter transformiert in

$$\frac{1}{\sqrt{2}} (|0\rangle|1\rangle - |1\rangle|1\rangle) \mapsto \frac{1}{\sqrt{2}} (|0\rangle|1\rangle - |1\rangle|0\rangle) = |\Psi^-\rangle. \tag{5.4}$$

⁴Allerdings ist das XOR irreversibel (es hat zwei Eingänge und einen Ausgang, der von beiden Eingängen abhängt). Das CNOT behält einen der beiden Eingänge (das control-Qubit). So wäre auch das XOR reversibel.

Die "Maschine" in Abb. 5.2 würde demnach aus einem Produktzustand ein maximal verschränktes EPR-Paar machen.

Da die Gatter reversibel sind, kann man es auch von rechts nach links lesen; man rechnet leicht nach, dass das CNOT die vier Bell-Zustände $|\Phi^+\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$ und $|\Psi^-\rangle$ auf die vier Produktzustände $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$ abbildet.

Gelänge also die Implementierung eines CNOT-Gatters, so könnte man die Bell-Zustände ganz einfach dadurch unterscheiden, dass man sie durch ein CNOT-Gatter schickt und dann die vier Zustände der Zwei-Qubit Standardbasis unterscheidet, was einfach zu bewerkstelligen ist. Leider ist die Umsetzung eines CNOT-Gatters mit photonischen Qubits sehr schwierig, weil die benötigte Photon-Photon-Wechselwirkung im nichtlinearen Medium extrem schwach ist.

Man kann sich bei Photonen jedoch das Phänomen der Interferenz zunutze machen. Es gibt Ansätze, den Mangel der nichtlinearen Interaktion zu umgehen, indem man zum Beispiel auf zusätzliche Hilfsphotonen zurückgreift [48]. Mit diesen Methoden kann man probabilistische Gatter implementieren, wobei die Fehlerwahrscheinlichkeit ungefähr umgekehrt proportional zum Aufwand an zusätzlichen Photonen ist. In letzter Zeit gelang es, durch Verwendung von zusätzlichen Einzelphotonen und bedingter Dynamik, probabilistische CNOT Gatter experimentell mit linearoptischen Mitteln zu realisieren [49, 50, 51].

5.4 Verschränkung in mehreren Freiheitsgraden

Wie dargelegt, können wir mit den verwendeten (passiven) linearoptischen Elementen maximal zwei der vier Bell-Zustände unterscheiden. Die zwei anderen geben uns stets ein anderes, drittes Ergebnis.

Um die Bell-Zustandsanalyse trotzdem durchführen zu können, machen wir uns zunutze, dass die Photonen aus unserer Quelle der spontanen parametrischen Fluoreszenz nicht nur polarisations- sondern auch in ihrer Energie bzw. Zeit verschränkt sind. Genau wie die Polarisationsverschränkung beruht diese Tatsache auf dem Entstehungsprozess der Paare (vgl. Abb. 4.1).

Der Entstehungszeitpunkt des SPF-Photonenpaares ist unsicher über die Kohärenzzeit des Pumplasers $\tau_c^p = 17$ ns – diese entspricht also der Kohärenzzeit des *Zwei*photonen-Wellenpakets. Weil die Kohärenzzeit des Lasers so lange, seine Energie also sehr genau definiert ist, ist die Summe der einzelnen Photonenenergien aufgrund der Energieerhaltung (Gl. 4.2) $E = \hbar(\omega_1 + \omega_2) = \hbar\omega_p$ ebenfalls sehr scharf definiert.

Die spektrale Breite der zwei Einzelphotonen ergibt sich aus dem Aufsammelprozess des Fluoreszenzlichts der SPF (siehe Kap. 4.2.2); die gesamte Bandbreite der SPF ist sehr groß [35]. Je nach Wahl der Einkoppeloptik kann so ein bestimmtes Spektrum ausgewählt

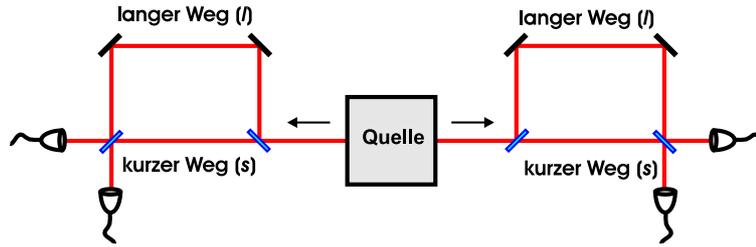


Abbildung 5.3: Aufbau zur Energie-Zeit Verschränkung nach FRANCON.

werden. Wie in Abb. 4.4 zu sehen ist, beträgt die Halbwertsbreite der in Koinzidenz gemessenen Einzelphotonspektren $\Delta\lambda_K \approx 2.5 \text{ nm}$, entsprechend einer Kohärenzzeit von

$$\Delta t \approx \frac{\lambda^2}{c \Delta\lambda} \approx 640 \text{ fs.} \quad (5.5)$$

Die Kohärenzzeit der Einzelphotonen ist also wesentlich kleiner als die Kohärenzzeit der gesamten Zweiteilchenwellenfunktion, $\tau_c^s \ll \tau_c^p$. Das bedeutet, dass der Zeitpunkt des Auftretens einer Detektion unscharf (τ_c^p) ist, die Zeitdifferenz zwischen der Detektion des einen und des anderen (einzelnen) Photons jedoch sehr gering (τ_c^s) ist.

Da in unserem Fall $\tau_c^s < 1 \text{ ps}$ gilt und damit weit unter der zeitlichen Auflösung der Messelektronik liegt, werden die zwei Photonen aus dem selben SPF-Prozess tatsächlich gleichzeitig – ”koinzident” – detektiert. Das gilt natürlich nur in dem Fall, dass die Photonen auf ihren (unterschiedlichen) Wegen durch Fasern, Luft, Glas, und so weiter den gleichen optischen Weg vom Entstehungspunkt (BBO-Kristall) bis zum Detektor zurücklegen⁵; außerdem müssen die Signallaufzeiten (z.B. in BNC-Kabeln) zwischen Teilen der Messapparatur und der Koinzidenzlogik bedacht werden (siehe dazu auch Kap. 5.5.5). FRANCON untersuchte solche zeitlichen Korrelationen 1989 und zeigte, dass sie zur Verletzung einer Bell-Ungleichung führen können, also nichtklassisch sind [52]. Da dieses Phänomen eine zentrale Rolle für meine vollständige Bell-Zustandsunterscheidung spielt, möchte ich die Idee, die dahinter steht, kurz erläutern. Der Aufbau dazu ist in Abb. 5.3 zu sehen.

Eine Quelle wie zum Beispiel unsere SPF-Quelle emittiere Energie-Zeit verschränkte Photonenpaare (zum Beispiel durch den zweistufigen Zerfall eines angeregten Atomzustandes mit langer Lebensdauer); das heißt, dass man den Zeitpunkt nicht (oder nur sehr ungenau) wissen kann. Die zwei Teilchen fliegen in entgegengesetzte Richtungen und durchlaufen je ein asymmetrisches Mach-Zehnder Interferometer. Jedes der beiden Photonen kann nun entweder den langen (”long”, l) oder den kurzen (”short”, s) Weg des Interferometers nehmen⁶. Wenn ein Teilchen kurz, das andere lang (also $s - l$ oder

⁵ *gleich* bedeutet hier mit einem Laufzeitunterschied der deutlich kleiner als das Koinzidenzzeitfenster ist. Das Koinzidenzzeitfenster gibt die maximale Zeitdifferenz an, die zwei Detektionsereignisse haben dürfen, um noch als ”gleichzeitig” interpretiert zu werden.

⁶ Ich bin mir der etwas flapsigen Sprechweise bewusst, bevorzuge sie jedoch der Anschaulichkeit halber.

$l-s$) läuft, können diese Fälle anhand der Ankunftszeiten an den Detektoren unterschieden werden. Wenn jedoch entweder beide kurz ($s-s$) oder beide lang ($l-l$) gelaufen sind, so lassen sich diese zwei Fälle $s-s$ und $l-l$ nicht unterscheiden, da nicht bekannt sein konnte, *wann* das Paar losgeschickt worden ist!

Essentiell wichtig bei diesem Phänomen ist, dass die Kohärenzzeit der Paare (die zeitliche Unsicherheit über die Emission τ_c aus der Quelle) größer als die zeitliche Trennung durch das Interferometer ist, da die Ereignisse $s-s$ und $l-l$ sonst unterscheidbar werden und nicht mehr kohärent sind. Das ist ganz analog der Kohärenzforderung bei Interferenzexperimenten in anderen Freiheitsgraden (z.B. im Ort).

Versuche dieser Art wurden durchgeführt und Interferenz zwischen den Zuständen nachgewiesen [53, 54]. SCARANI ET AL. hat ein Experiment vorgeschlagen [55], um Energie-Zeit Verschränkung nach FRANSON an durch kohärente Laserstrahlung erzeugten Quasipartikeln (Elektron-Loch Paaren) in Halbleiterbauelementen zu untersuchen.

Eine konzeptionell ähnliche, diskrete, Art der Energie-Zeit Verschränkung wurde von TITTEL [56] aufgezeigt ("time-bins"). Daneben gibt es Arbeiten, die statt der Polarisations- und Energie-Zeit Verschränkung Polarisations- und Impulsfreiheitsgrade der in spontaner parametrischer Fluoreszenz entstandenen Photonen verwenden [57].

Wie in Kap. 5.5.2 zu lesen ist, machen wir uns die Energie-Zeit Verschränkung der Photonen aus spontaner parametrischer Fluoreszenz zunutze, indem wir die – praktisch gleichzeitig entstandenen – einzelnen Photonen für *einen* Polarisationszustand, das heißt für nur *einen* Bellzustand, um einen Zeitbetrag separieren, der deutlich kleiner als die Kohärenzzeit der Gesamtwellenfunktion ist. Damit bleiben die "frühen" und "späten" Zustände kohärent, können interferieren und weiter in ihrer Polarisation analysiert werden. Man kann also sagen, dass wir die Information, die in den Polarisationszuständen kodiert und nach Kap. 5.2 mit linearoptischen Elementen nicht auslesbar ist, teilweise in einen anderen Freiheitsgrad (die zeitliche Korrelation der Photonen) "umkodieren", in dem sie uns zugänglich wird. Dadurch analysieren wir an einem Zustand, der in einen höheren Hilbertraum eingebettet ist. Mehr dazu in Kap. 5.5.2, wo ich erklären werde, wie diese Ideen experimentell umgesetzt werden.

5.5 Implementierung

In den folgenden Abschnitten werde ich darlegen, wie die vollständige Unterscheidung der Bell-Zustände mit linearen optischen Mitteln bewerkstelligt wird. Dabei machen wir uns bereits seit längerem bekannte und häufig angewendete Verfahren [58, 45, 37] zunutze, um zwei der Zustände eindeutig zu unterscheiden; daneben greifen wir auf die Verschränkung in anderen Freiheitsgraden (Kap. 5.4) unserer Photonenpaare zurück, um die letzten zwei Bell-Zustände ebenfalls identifizieren zu können [5].

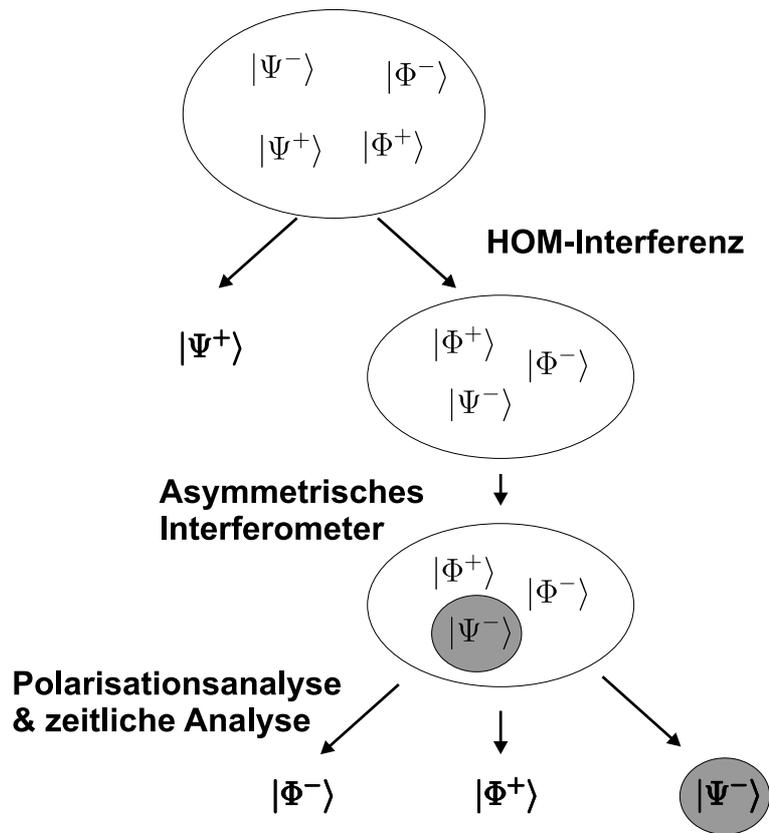


Abbildung 5.4: Schema der vollständigen Zustandsanalyse. Zur Erläuterung siehe Text. Die Photonen des grau hinterlegten Zustands $|\Psi^-\rangle$ werden im asymmetrischen Interferometer zeitlich separiert, die der zwei anderen dagegen nicht. Vergleiche mit Abb. 5.1.

Im Überblick kann der Ablauf der Zustandsdiskriminierung der polarisationskodierten Bell-Zustände wie folgt dargestellt werden (vgl. Abb. 5.4):

1. Ein Zustand ($|\Psi^+\rangle$) wird durch sein Verhalten bei Zweiphotoneninterferenz an einem Strahlteiler diskriminiert (Kap. 5.5.1). Die drei anderen Zustände verhalten sich hier gleich.
2. Ein zweiter Zustand ($|\Psi^-\rangle$) wird anhand seiner Polarisation in einem asymmetrischen Interferometer unterschieden. Dabei wird die Information, die in seiner Polarisation kodiert war, in den zeitlichen Freiheitsgrad umkodiert.
3. Die Zustände $|\Phi^-\rangle$ und $|\Phi^+\rangle$ können aufgrund der Energie-Zeit-Verschrankung nach dem asymmetrischen Interferometer in der P/M-Basis unterschieden werden.

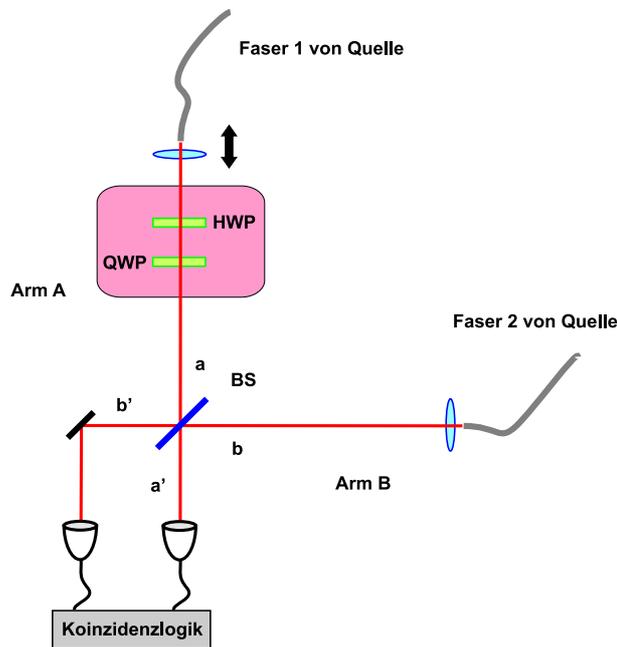


Abbildung 5.5: HOM-Interferenz am Strahlteiler (BS). Die zwei Moden der Arme A und B, in denen die SPF-Photonen propagieren, überlappen am Strahlteiler. Je nach Bell-Zustand verlassen beide Photonen den Strahlteiler in der selben, oder in unterschiedlichen Moden a' bzw. b'.

5.5.1 HOM-Interferenz

Das Prinzip

Im ersten Schritt der Zustandsanalyse machen wir uns die unterschiedlichen Symmetrieeigenschaften der Bell-Zustände unter Teilchenaustausch zunutze. Das Phänomen, auf dem der Effekt beruht, wurde erstmalig von HONG, OU und MANDEL untersucht [58] und nach ihnen benannt ("HOM"-Interferenz). Es handelt sich um die Zweiphotonen-Interferenz an einem Strahlteiler.

Da wir Zustände aus zwei Photonen, also Bosonen, betrachten, muss die Gesamtwellenfunktion in *allen* Quantenzahlen zusammen bosonischen Charakter haben, also unter Teilchenaustausch symmetrisch sein.

Betrachtet man die Bell-Zustände in Gl. 2.50-2.53, so kann man erkennen, dass nur der Zustand $|\Psi^-\rangle = |HV\rangle - |VH\rangle$ im Hilbertraum der Polarisationsfreiheitsgrade (Spin-Freiheitsgrade) antisymmetrisch ist. Folglich muss seine Ortswellenfunktion ebenfalls antisymmetrisch sein, um der Symmetrie der gesamten Wellenfunktion, dem Produkt aus Spin- und Ortswellenfunktion, Rechnung zu tragen. Die anderen drei Zustände haben symmetrische Spin- und Ortswellenfunktionen.

Lässt man die zwei räumlich getrennten Moden (a und b) der Bell-Zustands Photonen

an einem nichtpolarisierenden Strahlteiler (engl. "beam splitter", BS) überlappen (siehe Abb. 5.5), so werden sich die Photonen aufgrund eben besprochener Symmetrieeigenschaften unterschiedlich verhalten. Bei Zuständen mit bosonischer Ortswellenfunktion werden stets beide Photonen in die selbe Ausgangsmode transmittiert beziehungsweise reflektiert. Eine Messung zwischen den beiden Moden, a' und b', ergibt also für diese drei Zustände keine zeitlichen Koinzidenzen.

Für den Zustand mit antisymmetrischer, also fermionischer, Spin- und Ortswellenfunktion $|\Psi^-\rangle$ dagegen trennen sich die zwei Photonen immer am Strahlteiler auf und resultieren in je einem Photon in Mode a' und b'. Die Koinzidenzrate zwischen den Detektoren in den Moden a' und b' ist maximal, da jedes Photonenpärchen eine Koinzidenz auslöst. Wenn also eine Koinzidenz zwischen den Moden a' und b' auftritt, so können wir davon ausgehen, dass der Zustand der antisymmetrische war; beobachten wir keine Koinzidenz, so wissen wir nur, dass einer der drei anderen, symmetrischen, vorlag.

Wir können somit also genau *einen* Zustand identifizieren.

Wie in [36] genau beschrieben ist, tritt an dem verwendeten Strahlteiler ein unterschiedlicher Phasenschub zwischen horizontaler und vertikaler Polarisation in Reflexion auf⁷, der die Zustände $|\Psi^-\rangle$ und $|\Psi^+\rangle$ transformiert, bevor die Interferenz stattfindet. Das bewirkt, dass nicht mehr der Zustand $|\Psi^-\rangle$, sondern $|\Psi^+\rangle$ am Strahlteiler Koinzidenzen erzeugt, alle anderen nicht.

Nach dem Strahlteiler ist der der *einlaufende* Zustand $|\Psi^-\rangle$ jedoch in den Zustand $|\Psi^+\rangle$ transformiert. Um daran zu erinnern, dass ich den *transformierten* einlaufenden Zustand nach dem Strahlteiler meine, werde ich für diesen Zustand $|\Psi^-\rangle^{BS}$ (für "beam splitter") schreiben.

Der weitere Verlauf der Analyse wird davon nicht beeinflusst.

Experimentelle Umsetzung

Die Interferenz am Strahlteiler kann man nur beobachten, wenn die Einzelteilchenwellenfunktionen dort überlappen⁸. Zur Justage des räumlichen Modenüberlapps wurden die beiden Faserauskoppler (single-mode Faser mit Linse) in Haltern montiert, die die Translation als auch die Verkippung in beiden Richtungen senkrecht zum Strahl über Mikrometerschrauben erlauben.

Justiert habe ich dabei mithilfe eines mit bloßem Auge gut sichtbaren Diodenlasers bei etwa 700 nm, dessen Licht über einen Faserstrahlteiler in die Fasern in Abb. 5.5 eingekoppelt wurde. Überprüft man die Interferenz der Strahlen aus den Armen A und B in unmittelbarer Nähe hinter dem Strahlteiler sowie in einiger Entfernung (ca. 3 m),

⁷Dieser wird durch die dielektrischen Eigenschaften des Klebstoffes beeinflusst, der die zwei Prismen, die den Strahlteiler bilden, zusammenhält.

⁸PITTMAN ET AL. [59] haben darauf hingewiesen, dass es auch Interferenz geben kann, wenn die zwei einzelnen Photonen zu sehr unterschiedlichen Zeiten am Strahlteiler ankommen.

so kann man die Strahlen durch Verschiebung und Verkippung der Faserkoppler recht gut zum Überlapp bringen.

Dabei muss man beachten, dass die Strahlen in den beiden Armen gleich kollimiert sind (gleiche Krümmung der Wellenfronten); ansonsten leidet die Interferenz. Dazu wurde der Verlauf der Strahlprofile über eine große Distanz⁹ geprüft und dann über die Entfernung der Kopplerlinse zum Faserende versucht, die Strahltaile ins "unendliche" zu schieben. Dadurch wird die Aufweitung des Gaußschen Strahls minimal, also seine Rayleighlänge sehr groß.

Das spielt in diesem Experiment eine wichtige Rolle, da die Aufweitung der Strahlen bedingt, dass unterschiedlich weit gelaufene Strahlen unterschiedliche Strahlprofile haben und dann nicht mehr perfekt überlappen können. Dies würde insbesondere den Kontrast der Interferenz im asymmetrischen Interferometer (Kap. 5.5.2) drastisch reduzieren: dort lassen wir Strahlteile absichtlich unterschiedlich weit propagieren, um einen Zeitunterschied zu erzeugen.

Es stellte sich heraus, dass ein guter Kontrast der HOM-Interferenz (jenseits der 90%) sehr schwer zu justieren war, was mit Sicherheit daran liegt, dass hierbei sowohl die Photonenspektren, als auch ihr räumlicher Überlapp, als auch Imperfektionen der Polarisation – also der Bell-Zustands Präparation – einen Beitrag leisten.

Neben der Justierung des beschriebenen (transversalen) Modenüberlapps muss man dafür Sorge tragen, dass die Einteilchenwellenfunktionen auch longitudinal überlappen: Da keine Interferenz auftritt, wenn die Wellenfunktionen nicht überlappen, teilen sich die Photonen in diesem Fall zufällig auf die Moden a' und b' auf. Bei perfektem Überlapp würden wir für $|\Psi^+\rangle$ eine Verdopplung der Koinzidenzrate erwarten; für die drei anderen Bell-Zustände erwarten wir keine Koinzidenzen mehr, wenn die Wellenfunktionen überlappen.

Nach den Überlegungen in Kap. 4.4 erwarten wir eine Kohärenzzeit von etwa $\tau_c^s \approx 650$ fs. Das bedeutet, dass der optische Weg der Photonen vom Entstehungspunkt (im Mittel das Zentrum des BBO-Kristalls, da $c\tau_c^p \gg 2$ mm Kristalllänge ist) zum Strahlteiler auf einen Bruchteil von $c\tau_c^s \approx 0.2$ mm genau gleich sein muss.

Dazu wurde der optische Weg (durch Luft und Fasern) gemessen bzw. berechnet¹⁰ und die Faserkoppler in Arm 1 und 2 so aufgestellt, dass der Unterschied weniger als $O(1\text{cm})$ betrug. Der Faserkoppler in Arm 1 wurde auf eine motorgesteuerte Translationsstufe montiert, die eine Längenanpassung des Arms im Mikrometerbereich über etwa ± 1.2 cm erlaubt. Wenn der optische Weg in beiden Armen genau gleich ist, kann man die Interferenz beobachten.

⁹circa 8 m; die Weglängen im experimentellen Aufbau sind kleiner als 4 m.

¹⁰Der Brechungsindex des Faserkerns ist $n \approx 1.5$

Zum Auffinden der richtigen Position der Translationsstufe stellte ich zunächst durch das Halb- und Viertelwellenplättchen in Abb. 5.5 den Zustand $|\Psi^-\rangle$ ein. Diesen kann ich über die Polarisationsmessungen, die in Kap. 4.5.2 beschrieben sind, nachweisen.

Die zwei Wellenplättchen müssen unbedingt *vor* der Justage des räumlichen Überlapps in den Strahlengang gestellt werden, da sie aufgrund ihrer endlichen Dicke einen Strahlversatz bewirken und wegen eines eventuellen kleinen Keils den Strahl auch aufweiten und ablenken können. Der Effekt eines Keils macht sich besonders dann bemerkbar, wenn die Plättchen zum Wechsel zwischen den verschiedenen Zuständen gedreht werden. Der Kontrast der HOM-Interferenz ist dann für verschiedene Bell-Zustände unterschiedlich stark, weil der (transversale) Modenüberlapp unterschiedlich gut ist.

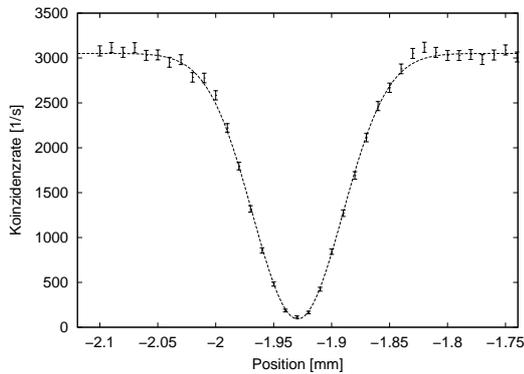
Die Wellenplättchen verschieben aber auch die longitudinale Position des maximalen Überlapps, weil der Brechungsindex und damit die optische Weglänge des doppelbrechenden Materials nicht identisch dem der Luft ist.

Da nur die Position für maximale Interferenz, nicht aber der Kontrast der Interferenz beeinflusst wird, ist das nicht weiter schlimm. Die optimale Position musste ohnehin nach jeder Justage neu bestimmt werden, da sie sich zum Beispiel durch die geöffneten und wieder geschlossenen Steckverbindungen zwischen Fasern geringfügig aber merklich verändern kann.

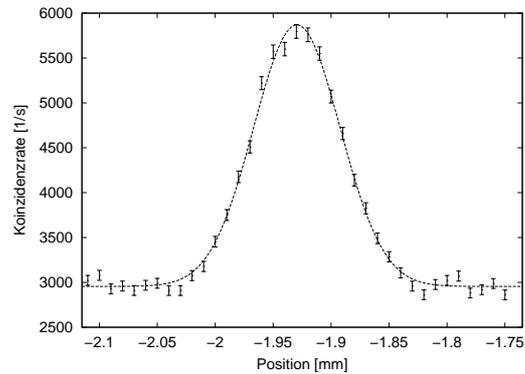
In Abb. 5.6 kann man deutlich den so genannten "dip", also die Abnahme der Koinzidenzrate für die Zustände $|\Psi^-\rangle$, $|\Phi^-\rangle$ und $|\Phi^+\rangle$ erkennen. Der Zustand $|\Psi^+\rangle$ zeigt die erwartete starke Zunahme ("peak") der Koinzidenzrate.

Die Kontraste¹¹ lagen bei $(94.3 \pm 0.5)\%$ für $|\Psi^-\rangle$, $(92.4 \pm 0.6)\%$ für $|\Phi^-\rangle$ und $(95.3 \pm 0.5)\%$ für $|\Phi^+\rangle$. Die Koinzidenzrate hat sich beim Zustand $|\Psi^+\rangle$ innerhalb des statistischen Fehlers verdoppelt¹². Die Halbwertsbreite der gaußförmigen Verläufe ist bei allen Zuständen praktisch gleich und beträgt etwa $89 \mu\text{m} = 297 \text{ fs} \cdot c^{13}$.

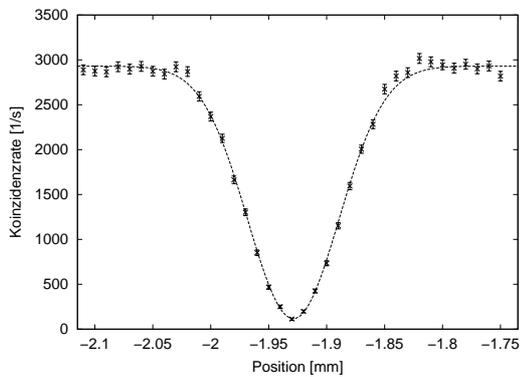
Wir lassen den Faserkoppler in der Position, wo die Extrema sind, und können somit $|\Psi^+\rangle$ durch das Ereignis "je ein Photon in Mode a' und b'" unterscheiden. Dass die Kontraste nicht perfekt sind, könnte neben den oben angeführten Gründen auch daran liegen, dass der Strahlteiler nicht exakt gleiche Reflexion und Transmission für alle Polarisierungen und Eingangsmoden aufweist [58].



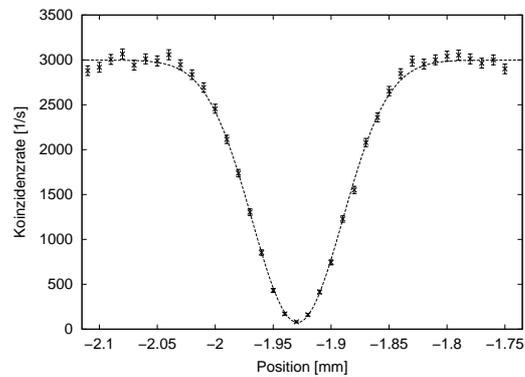
(a) Koinzidenz-dip für den Zustand $|\Psi^-\rangle$



(b) Koinzidenz-peak für den Zustand $|\Psi^+\rangle$



(c) Koinzidenz-dip für den Zustand $|\Phi^-\rangle$



(d) Koinzidenz-dip für den Zustand $|\Phi^+\rangle$

Abbildung 5.6: HOM-Interferenz

5.5.2 Das asymmetrische Interferometer

Nach der HOM-Interferenz finden wir für die einlaufenden Zustände $|\Psi^-\rangle$, $|\Phi^-\rangle$ und $|\Phi^+\rangle$ zwei Photonen in der Mode $i=b'$ (siehe Abb. 5.5).

Diese durchlaufen nun das Interferometer, das aus einem polarisierenden¹⁴ Strahlteiler (PBS) und zwei Prismen besteht. Diese Anordnung, wie sie in Abb. 5.7 zu sehen ist,

¹¹siehe Anhang A.1.

¹²der "peak-to-peak" Kontrast zwischen $|\Psi^-\rangle$ und $|\Psi^+\rangle$ beträgt $(97 \pm 1)\%$.

¹³Der hier gemessene Wert der Kohärenzzeit weicht von dem aus den Spektren berechneten ab. Das kann daran liegen, dass sich die Einkopplung der Fluoreszenzmoden leicht geändert hat.

¹⁴Ein polarisierender (50-50) Strahlteiler transmittiert horizontal polarisierte Photonen und reflektiert vertikal polarisierte Photonen; genauer siehe unten.

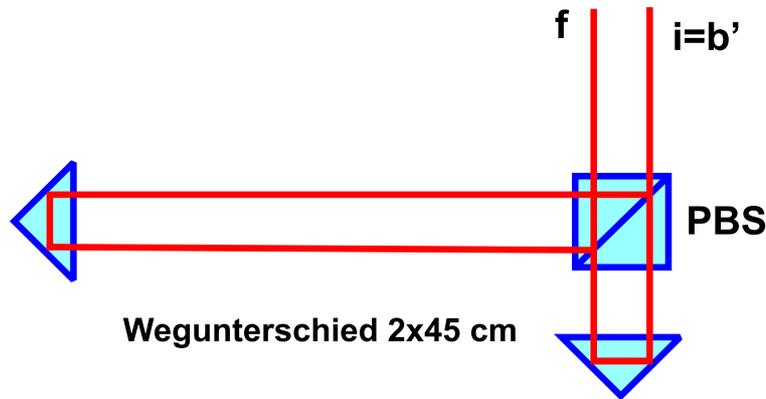


Abbildung 5.7: Das asymmetrische Interferometer mit Eingangsmode i vom HOM-Interferenz Strahlteiler.

macht es leichter, das Interferometer zu justieren, da der Strahlengang unabhängig von einer Drehung der Prismen um die Senkrechte ist ("Katzenaugen-Prinzip"). Die hin- und rücklaufenden Strahlen sind immer parallel, sodass ein Strahlteiler ausreicht.

Daneben ist es stabiler als die übliche Mach-Zehnder Anordnung (Abb. 5.3). Der für uns entscheidende Vorteil dieser Anordnung ist aber, dass die Länge eines Interferometerarms durch Verschieben *eines* optischen Elements (z.B. das Prisma im langen Arm) verändert werden kann.

Alle verwendeten Elemente sind anti-reflex beschichtet bei 702 nm. Der Überlapp der Moden aus dem langen und dem kurzen Arm, resultierend in Mode f , wurde wiederum an zwei entfernten Punkten kontrolliert.

Der lange Arm ist circa 45 cm länger als der kurze. Der polarisierende Strahlteiler transmittiert horizontal und reflektiert vertikal polarisierte Teile der Wellenfunktion. Das bedeutet, dass die Amplitude vertikaler Polarisation des einfallenden Zweiteilchenzustands erstens um etwa $2 \cdot 45 \text{ cm}/c \approx 3 \text{ ns} =: \Delta t$ gegenüber der horizontaler Polarisation verzögert wird; und zweitens tritt ein Phasenfaktor $e^{i\gamma}$ zwischen horizontaler und vertikaler Polarisationsamplitude auf. Dieser rührt daher, dass der Weglängenunterschied zwischen (s) und (l) im Allgemeinen nicht genau einem ganzzahligen Vielfachen der Wellenlänge entspricht.

Die Wirkung des Interferometers U_{IF} kann also wie folgt beschrieben werden:

$$\begin{aligned}
 U_{IF} : \quad |H\rangle_i &\mapsto |Hs\rangle_f \\
 |V\rangle_i &\mapsto e^{i\gamma} |Vl\rangle_f,
 \end{aligned}
 \tag{5.6}$$

wobei " s " und " l " daran erinnern, dass die Zustände den kurzen (s) beziehungsweise den langen (l) Arm genommen haben. An dieser Stelle wird also Information, die in der Polarisation kodiert ist, zusätzlich in einem anderen Freiheitsgrad – der Zeit – kodiert.

Die drei Zustände $|\Psi^-\rangle^{BS}$, $|\Phi^-\rangle$ und $|\Phi^+\rangle$ erfahren im Interferometer die Transformation $U_{IF} \otimes U_{IF}$, da ja beide Photonen in der gleichen Mode i sind. Die Berechnung nach Gl. 5.6 ist sehr einfach und ergibt

$$\begin{aligned} |\Psi^-\rangle^{BS} &= \frac{1}{\sqrt{2}} (|H\rangle_i |V\rangle_i + |V\rangle_i |H\rangle_i) \mapsto \frac{e^{i\gamma}}{\sqrt{2}} (|Hs\rangle_f |Vl\rangle_f + |Vl\rangle_f |Hs\rangle_f) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|H\rangle_i |H\rangle_i - |V\rangle_i |V\rangle_i) \mapsto \frac{1}{\sqrt{2}} (|Hs\rangle_f |Hs\rangle_f - e^{i2\gamma} |Vl\rangle_f |Vl\rangle_f) \\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|H\rangle_i |H\rangle_i + |V\rangle_i |V\rangle_i) \mapsto \frac{1}{\sqrt{2}} (|Hs\rangle_f |Hs\rangle_f + e^{i2\gamma} |Vl\rangle_f |Vl\rangle_f) \end{aligned} \quad (5.7)$$

Die transformierten Zustände nenne ich $|\Psi^-\rangle^{\text{IF}}$, $|\Phi^-\rangle^{\text{IF}}$ und $|\Phi^+\rangle^{\text{IF}}$.

Die zwei Photonen des Zustandes $|\Psi^-\rangle^{\text{IF}}$, die in dieser Basis ja in der Polarisation anti-korreliert sind, würden nun also mit einer zeitlichen Verzögerung Δt detektiert werden. Die Photonen der Zustände $|\Phi^\pm\rangle^{\text{IF}}$ sind in der Polarisation korreliert, würden also gleichzeitig detektiert werden, da beide Photonen entweder den kurzen oder den langen Weg gelaufen sind.

Erinnern wir uns (vgl. Kap. 5.5.1), dass die einzelnen Photonen wegen der Energie-Zeit Verschränkung gleichzeitig, das heißt mit einem Zeitunterschied τ_c^s unter 10^{-3} ns, am ersten Strahlteiler (BS) ankamen und damit auch gleichzeitig in das Interferometer gelangen. Die Verzögerung, die dann im Interferometer auftritt, ist also wesentlich größer als die Kohärenzzeit der einzelnen Photonen:

$$\tau_c^s \ll \Delta t \quad (5.8)$$

Einzelphotoneninterferenz haben wir also nicht zu erwarten [52, 54]. Wesentlich ist aber, dass für die Zustände $|\Phi^\pm\rangle$ wegen der Energie-Zeit Verschränkung die Kohärenzzeit der Paarwellenfunktion der Kohärenzzeit des Pumplasers τ_c^p entspricht und deswegen mit 17 ns größer als die zeitliche Trennung Δt ist:

$$\Delta t < \tau_c^p. \quad (5.9)$$

Aus diesem Grund sind die ihre zeitlich getrennten Amplituden (s bzw. l) nach dem Interferometer immer noch kohärent und können somit interferieren. Man beachte, dass die Zustände $|\Phi^\pm\rangle$ in der H/V-Basis des PBS korreliert sind, dass also beide Photonen immer den selben Weg (s oder l) nehmen.

5.5.3 Analyse in P/M-Basis

Nachdem der Zustand $|\Psi^-\rangle$ durch seine Polarisations-Antikorrelation im Interferometer sozusagen "markiert" worden ist, indem man seine zwei Photonen immer zu unterschiedlichen Zeitpunkten t und $t + \Delta t$ detektieren wird, bleibt die Unterscheidung der Zustände $|\Phi^-\rangle$ und $|\Phi^+\rangle$.

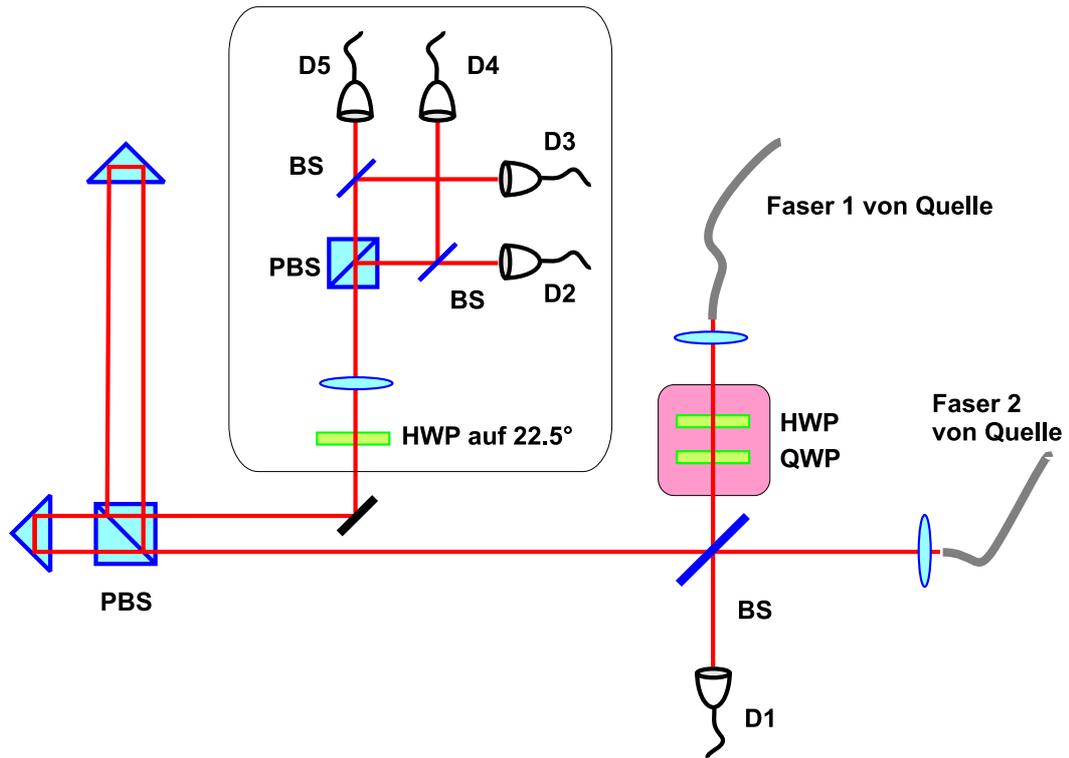


Abbildung 5.8: Der gesamte Aufbau zur Analyse; die Polarisationsanalyse in P/M-Basis ist markiert. Das Wellenplättchen macht den Basiswechsel, die Linse ($f=12$ cm) fokussiert die Photonen in die Detektoreinheit.

Diese zeigen in der P/M-Basis unterschiedliche Korrelationen (vgl. Gl. 2.57), zur Erinnerung

$$\begin{aligned}
 |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|PP\rangle + |MM\rangle) \\
 |\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|PM\rangle + |MP\rangle).
 \end{aligned}
 \tag{5.10}$$

Wir analysieren die drei Zustände aus Gl. 5.7 deswegen in P/M-Basis, indem wir sie zunächst durch ein Halbwellenplättchen auf 22.5° laufen lassen, welches den Basiswechsel macht, und dann in H/V-Basis analysieren. Das Wellenplättchen transformiert

$$\begin{aligned}
 U_{\lambda/2}(22.5^\circ) : |H\rangle &\mapsto |P\rangle = (|H\rangle + |V\rangle)/\sqrt{2} \\
 |V\rangle &\mapsto |M\rangle = (|H\rangle - |V\rangle)/\sqrt{2},
 \end{aligned}
 \tag{5.11}$$

und zwar unabhängig vom Fall (s) oder (l). Alle Zustände befinden sich in der selben Mode f .

Damit sehen die Zustände aus Gl. 5.7 mit der relativen Interferometerphase $\gamma = 0$ nach dem Wellenplättchen so aus (Modenindex f und globale Phase weggelassen):

$$\begin{aligned}
|\Psi^-\rangle^{\text{IF}} &\mapsto |\Psi^-\rangle^{\text{WP}} = \\
\frac{1}{2\sqrt{2}} &[(|HH\rangle - |VV\rangle)(|sl\rangle + |ls\rangle) + (|VH\rangle - |HV\rangle)(|sl\rangle - |ls\rangle)] \\
|\Phi^\pm\rangle^{\text{IF}} &\mapsto |\Phi^\pm\rangle^{\text{WP}} = \\
\frac{1}{2\sqrt{2}} &[(|HH\rangle + |VV\rangle)(|ss\rangle \pm |ll\rangle) + (|HV\rangle + |VH\rangle)(|ss\rangle \mp |ll\rangle)] \quad (5.12)
\end{aligned}$$

Hierbei habe ich die Information, ob die Amplitude zum langen oder zum kurzen Weg gehört, wegen der besseren Lesbarkeit in Form eines "Kets" anhängt.

Wie erwähnt, sind wegen der Energie-Zeit Verschränkung Zweiteilchenamplituden der Form $|XsYs\rangle$ und $|XlYl\rangle$ kohärent, wo $X, Y \in \{H, V\}$, da die Trennung zwischen s und l kleiner als die Kohärenzlänge ist. Deswegen können die Amplituden interferieren, und die Zustände $|\Phi^\pm\rangle^{\text{IF}}$ vereinfachen sich zu

$$\begin{aligned}
|\Phi^+\rangle^{\text{WP}} &= \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle) \\
|\Phi^-\rangle^{\text{WP}} &= \frac{1}{\sqrt{2}} (|HV\rangle + |VH\rangle) \quad (5.13)
\end{aligned}$$

Nach dem darauf folgenden polarisierenden Strahlteiler werden die zwei Photonen des Zustandes $|\Phi^-\rangle^{\text{WP}}$ *gleichzeitig* und in verschiedenen Ausgangsmoden detektiert. Der Zustand $|\Phi^+\rangle^{\text{WP}}$ resultiert in zwei ebenfalls *gleichzeitigen* Ereignissen, jedoch mit zwei Photonen in der selben Ausgangsmode.

Diese zwei Photonen in der selben Mode können mit 50% Wahrscheinlichkeit mit Hilfe eines Strahlteilers in zwei verschiedenen Detektoren nachgewiesen werden (vgl. Kap. 4.3). Ansonsten werden sie als Einzelphotonenereignis verworfen.

Folgende Tabelle zeigt, welche Detektorkombinationen zu welchem Bell-Zustand gehören. Die Nummerierung der Detektoren/Photodioden ist in Abb. 5.8 zu sehen.

Zustand	Detektorkombinationen
$ \Psi^-\rangle$	alle $s - l$ Kombinationen von D2-D5
$ \Psi^+\rangle$	D1(s) und einer von D2-D4 (s oder l)
$ \Phi^-\rangle$	D2 und (D3 oder D5); D4 und (D3 oder D5). nur gleichzeitig
$ \Phi^+\rangle$	D2 und D4; D3 und D5. nur gleichzeitig

Tabelle 5.1: Detektorkombinationen für die vier Bell-Zustände.

5.5.4 Die Detektoreinheit

Zur Polarisationsanalyse hinter dem asymmetrischen Interferometer kommt das in Anhang A.4 dargestellte Modul zum Einsatz. Es beinhaltet den polarisierenden Strahlteiler, die zwei nichtpolarisierenden Strahlteiler zur (probabilistischen) Detektion von zwei Photonen in einer Mode, und vier Avalanche-Photodioden. Außerdem ist die gesamte Elektronik zur Spannungsversorgung der Dioden, sowie zur digitalen Signalerzeugung integriert.

Ausgangssignale

Trifft ein Photon auf die aktive Fläche einer Photodiode, so wird, wie schon in Kap. 4.3 erwähnt, ein Spannungspuls erzeugt, der mit einer in diesem Fall einstellbaren Schwellenspannung verglichen wird. Übersteigt der Puls die Schwellenspannung, wird am Ausgang des Moduls ein digitaler NIM-Puls für diese Diode erzeugt. Da die Flanke des Diodenpulses eine endliche Steigung hat, hängt der Auslösezeitpunkt von der Höhe der Schwelle ab.

Die Ankunftszeiten der $s - l$ Ereignisse – verursacht durch das asymmetrische Interferometer – liegen nur $\Delta t = 3$ ns auseinander. Daher war es notwendig, die Schwellenspannungen der vier Dioden so einzustellen, dass die von gleichzeitig ankommenden Photonen ausgelösten NIM-Signale ebenfalls gleichzeitig das Detektormodul verlassen. Dabei darf sich die Einzelzählrate der Diode nicht ändern.

In Abb 5.9 sieht man die zeitliche Verteilung der NIM-Signale der Detektoren D2 bis D4. Bei dieser Messung (mit einem 1 GHz-Digitaloszilloskop von LeCroy erstellt) sind sowohl $s - s$ als auch $s - l$ Ereignisse erfasst.

Für diese Messung wurde der verschiebbare Faserkoppler (siehe Kap. 5.5.1) in eine Position gebracht, in der keine HOM-Interferenz mehr auftritt, die Photonenpaare sich also statistisch am Strahlteiler aufteilen. Es werden nur solche Ereignisse registriert, bei denen sich das Paar aufteilt. Die Detektion des Photons an D1 definiert den Nullpunkt der Messung ("Trigger").

Ein Photon, das den kurzen Arm des Interferometers genommen hat, sollte im Modul gleichzeitig mit dem anderen im Detektor D1 registriert werden. Eines, das den langen Arm genommen hat, um $\Delta t = 3$ ns später. Wegen des Halbwellenplättchens auf 22.5° vor der Einheit sieht jede Diode s - und l -Ereignisse¹⁵.

Die unterschiedliche Höhe der Maxima kommt von unterschiedlichen Messzeiten und damit unterschiedlicher Anzahl von Ereignissen pro Diode. Man erkennt, dass – nach

¹⁵Ohne dem Wellenplättchen könnten D2/D4 wegen der polarisierenden Strahlteiler nur l -Photonen sehen und D3/D5 nur s -Photonen; das Wellenplättchen dreht H/V linear polarisiertes Licht auf $\pm 45^\circ$ linear polarisiertes Licht.

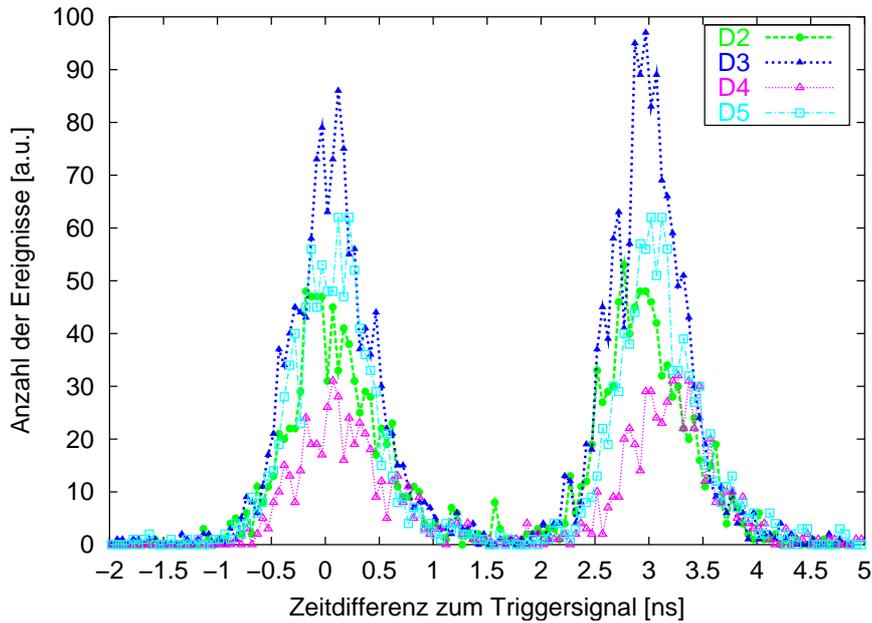


Abbildung 5.9: Zeitliche Verteilung der Detektorsignale von D2-D5. Die Unterschiedlichen Höhen der Graphen für die Detektoren D2-D5 kommen von unterschiedlichen Messzeiten.

der Anpassung der Schwellenspannungen – die Maxima für Photonen, die den kurzen Weg gelaufen sind, recht gut übereinanderliegen; das selbe gilt für diejenigen Ereignisse, bei denen die Photonen den langen Weg genommen haben.

Die Maxima liegen auf ungefähr 200 ps genau übereinander. Der Zeitunterschied zwischen den $s - l$ Ereignissen beträgt bei jedem Detektor (3.0 ± 0.1) ns.

Die Maxima der s -Ereignisse liegen nicht genau bei 0 ns. Deswegen wurde das NIM-Signal vom externen Detektor D1 mit einer einstellbaren NIM-delay- Stufe relativ zu den Dioden (D2-D5) verzögert.

Wegen der relativ großen Breite von etwa $\text{FWHM} \approx (0.8 \pm 0.15)$ ns der Maxima bei einer Trennung von nur 3.0 ns könnte man die Unterscheidung von gleichzeitigen und nichtgleichzeitigen Ereignissen sicher verbessern, indem man den langen Interferometerarm noch länger machen würde, um so den Überlapp der s -Ereignisse mit den l -Ereignissen zu minimieren.

Dabei muss man beachten, dass dadurch der Überlapp der s bzw. l -Moden, und damit auch die Interferenz nach dem Interferometer schlechter würde. Da der einlaufende Strahl eine – wenn auch nur geringe – Divergenz aufweist, erfahren die Teilstrahlen im langen und kurzen Arm nämlich unterschiedlich starke Aufweitung. Das mindert den Kontrast

der Interferenz.

Durchbruch-Fluoreszenz der Dioden

Jedes Mal, wenn ein Photon in einer Avalanche-Photodiode (APD) einen kontrollierten Durchbruch, eine Ladungslawine, auslöst, werden dabei von der Diode Fluoreszenzphotonen emittiert. Aufgrund der engen Anordnung der vier Photodioden in dem Detek-

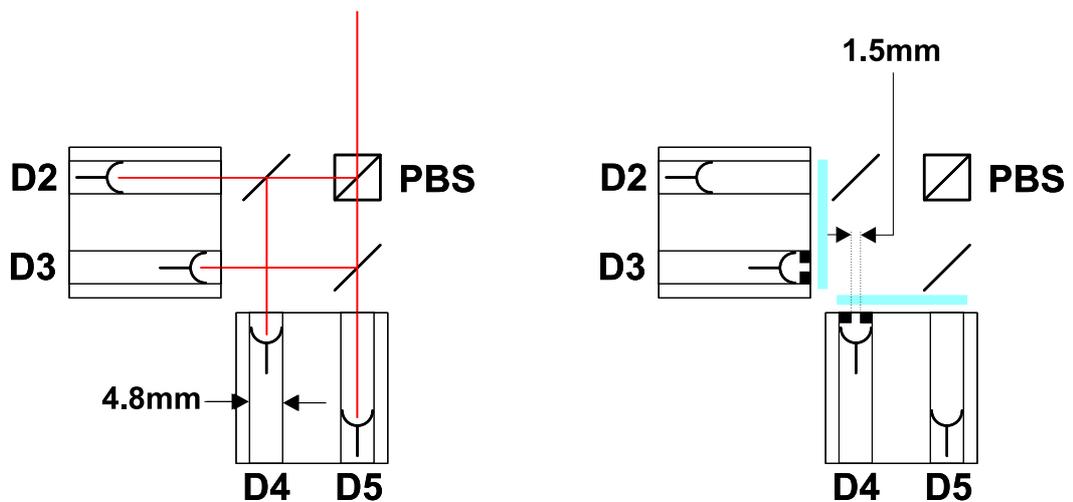


Abbildung 5.10: Links: Strahlverlauf (rot) und Lage der Avalanche-Dioden in der Detektoreinheit. Rechts: Blenden vor Dioden D3 und D4 sowie Filter (blau) zur Unterdrückung von Koinzidenzen durch Durchbruch-Fluoreszenz.

tormodul (siehe Abb. 5.10, links), konnte beobachtet werden, dass solche Fluoreszenzphotonen, erzeugt durch die Detektion eines Einzelphotons in einer Diode, den Weg zu einer anderen Diode fanden und dort ebenfalls ein Detektionsereignis auslösten.

Zur besseren Kühlung durch Peltier-Elemente stecken die vier Dioden in den Bohrungen zweier Aluminiumblöcke. Diese Bohrungen haben einen Durchmesser von 4,8 mm. Um die Weglängen der zu detektierenden Photonen vom polarisierenden Strahlteiler zu den Dioden für alle Dioden exakt gleich lang zu machen, wurden die Dioden D2 und D3 weiter vorne im Alu-Block angebracht.

Diese zwei Dioden "sehen" also einen wesentlich größeren Raumwinkel als die Dioden D1 und D4, die weiter hinten in den Bohrungen angebracht sind. Die durch die Bohrungen entstandenen Kanäle wirken hier wie Raumfilter¹⁶.

¹⁶Für die Detektion der von außen in das Detektormodul fokussierten Bell-Zustands-Photonen spielt das keine Rolle, da sie sowieso in einer wohldefinierten, kollimierten Mode zur Diode laufen.

Die Durchbruch-Photonen werden von der Diodenfläche (0.5 mm Durchmesser) in einen großen Raumwinkel emittiert. Deswegen ist die Kopplung zwischen den Dioden D2 und D3 für diese Photonen am größten. Tatsächlich zeigten Koinzidenzanalysen, dass diese zwei Dioden am stärksten übersprechen.

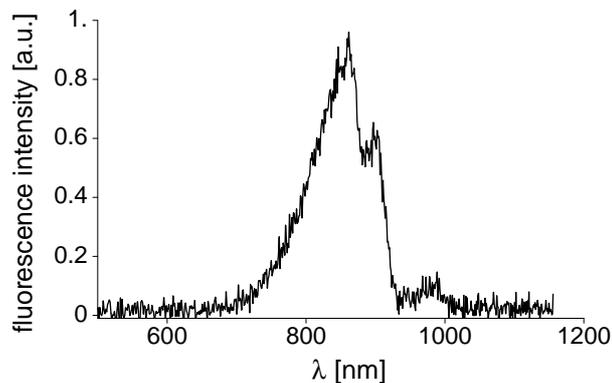


Abbildung 5.11: Spektraler Verlauf der Durchbruch-Fluoreszenz nach [60]. Bei der Wellenlänge der Bell-Zustands-Photonen, 702 nm, treten fast keine Fluoreszenzphotonen auf.

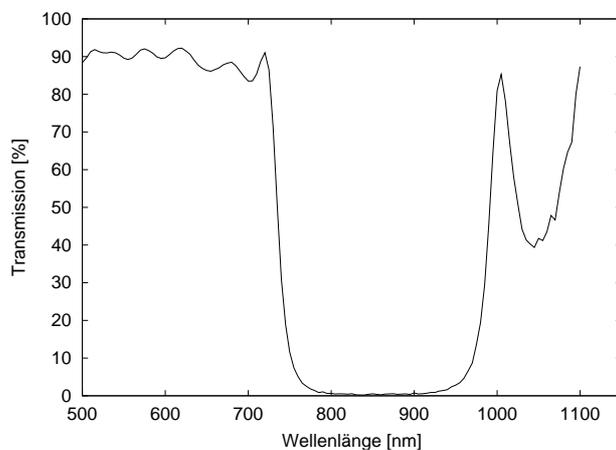


Abbildung 5.12: Transmissionsverlauf der verwendeten Filter in der Detektoreinheit. Bei 702 nm ist die Transmission noch etwa 84%.

Durch diesen Mechanismus werden künstliche "Koinzidenzen" erzeugt. Unglücklicherweise entspricht der zeitliche Unterschied zwischen der Detektion des einen Photons und der Detektion des anderen (Durchbruch-) Photons recht genau den $\Delta t = 3$ ns, die in meinem Experiment die *s*- und *l*- Photonen getrennt sind [60].

Durch die Diodenfluoreszenz werden also früh-spät Ereignisse künstlich erzeugt, die dem Zustand $|\Psi^-\rangle$ zugeordnet würden, obwohl nur gleichzeitige ($|\Phi^\pm\rangle$) oder einzelne Photonen in das Detektormodul gelangen.

Um diese früh-spät Koinzidenzen loszuwerden, versah ich die Kanäle der Dioden D3 und D4 mit genau angepassten Aluminium-Blenden, die den Kanal auf einer Länge von etwa 4mm auf 1.5 mm Durchmesser verengen (vgl. 5.10, rechts). Dadurch konnte ein Großteil der ungewünschten Ereignisse zwischen diesen zwei Dioden eliminiert werden.

Zusätzlich stellte ich vor die Öffnungen der Aluminiumblöcke Filter, deren spektraler Transmissionsverlauf dem Fluoreszenzspektrum der Durchbruch-Photonen angepasst ist. Dieses Spektrum ist an Abb. 5.11 zu sehen. Die Filtertransmission zeigt Abb. 5.12. Der Einsatz der Filter war überhaupt nur möglich, da wir nach Abb. 5.11 fast keine Durchbruch-Photonen bei 702 nm zu erwarten haben. Hier ist die Transmission der Filter etwa 84%. Das breite spektrale Maximum der Diodenfluoreszenz bis etwa 950 nm wird fast vollständig unterdrückt.

5.5.5 Die Koinzidenzeinheit

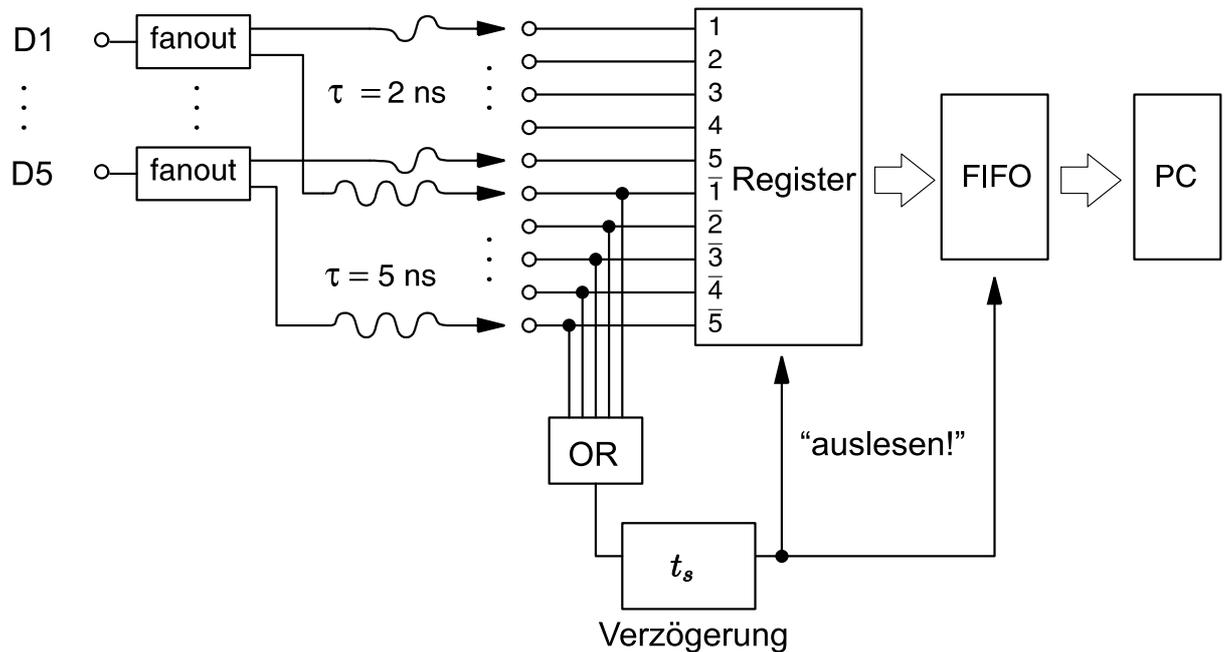


Abbildung 5.13: Verarbeitung der Koinzidenzsignale (siehe Text).

Um die vier Bell-Zustände unterscheiden zu können, müssen gleichzeitige, sowie "früh-spät"-Ereignisse, also um $\Delta t = 3 \text{ ns}$ verzögerte, Koinzidenzen erkannt werden (vgl. Tabelle 5.1).

Zu diesem Zweck werden die Signale, die von den Detektoren D1 bis D5 kommen (vgl. Abb. 5.8), zunächst durch ein "fanout" kopiert. Eine der je zwei Signalkopien wird gegenüber der anderen um 3 ns über ein NIM-Kabel verzögert. Von jedem Detektorsignal liegt dann also das "Original" und eine um 3 ns verzögerte Kopie vor (siehe Abb. 5.13). Diese $2 \times 5 = 10$ digitalen Signale liegen dann in der Koinzidenzeinheit als Eingangssignale mit Index

$$1, 2, \dots, 5, \bar{1}, \bar{2}, \dots, \bar{5}$$

in einem Register an. Der Strich über den Zahlen erinnert daran, dass das Signal um 3 ns verzögert wurde.

Sobald mindestens eine der verzögerten (digitalen) Signalleitungen $\bar{1}, \bar{2}, \dots, \bar{5}$ *High* wird, wird der Inhalt *aller zehn* Signalleitungen aus dem Register in einen FIFO-Puffer weitergegeben. Von dort aus werden sie in einen Rechner eingelesen¹⁷. Das Auslesen des Registers in den FIFO-Puffer wird dabei um eine kleine Zeitspanne t_s verzögert. Diese Zeitspanne bestimmt, um welche Zeit die Signale von zwei Detektoren maximal voneinander abweichen dürfen, um noch als *gleichzeitig* klassifiziert zu werden.

Abb. 5.14 verdeutlicht die Funktionsweise der Koinzidenzeinheit. Es sind Zweiphotonenereignisse dargestellt, bei denen nur vier Kanäle interessieren; die anderen Kanäle bleiben *Low*.

Nach einer Wartezeit von t_s nach der (in dieser schematischen Darstellung) steigenden Flanke des verzögerten Signals $\bar{1}$ werden alle Kanäle ausgelesen.

Wurden die Signale beider Detektoren D1, D2 von gleichzeitigen ($s - s$ oder $l - l$) Photonen ausgelöst (Abb. 5.14, oben), so sind beim Zeitpunkt des Auslesens alle vier Leitungen ($1, \bar{1}, 2, \bar{2}$) *High*. Das entsprechende Bitmuster, das im Rechner das Ereignis charakterisiert, ist rechts daneben zu sehen.

Wurden die Signale jedoch von einem ($s - l$) Ereignis¹⁸, also von zwei um $\Delta t = 3$ ns zeitlich getrennten Photonen ausgelöst, und nehmen wir an, an D1 komme das erste an (Abb. 5.14, unten), so kann das verzögerte Signal $\bar{2}$ des zweiten Photons bis zum Auslesezeitpunkt nicht am Register angekommen sein.

Es werden also nur die zwei Leitungen $1, \bar{1}$ des ersten Photons, und die nicht verzögerte Leitung 2 des zweiten Photons, als *High* in den FIFO-Puffer gespeichert. Die Leitung $\bar{2}$ bleibt *Low*.

Wir sehen also, dass die zwei Bits des zuerst signalisierenden Detektors immer beide gesetzt werden. Je nachdem, ob der zweite Detektor "gleichzeitig" oder "später" auslöst, sind entweder beide Bits gesetzt, oder nur das der nicht verzögerten Leitung.

¹⁷Der FIFO-Puffer hat eine "Totzeit" von etwa 15 ns, in der er die Daten speichert.

¹⁸($s - l$)- und ($l - s$)-Ereignisse sind äquivalent, werde sie also nicht mehr extra angeben; genauso ($s - s$) und ($l - l$)

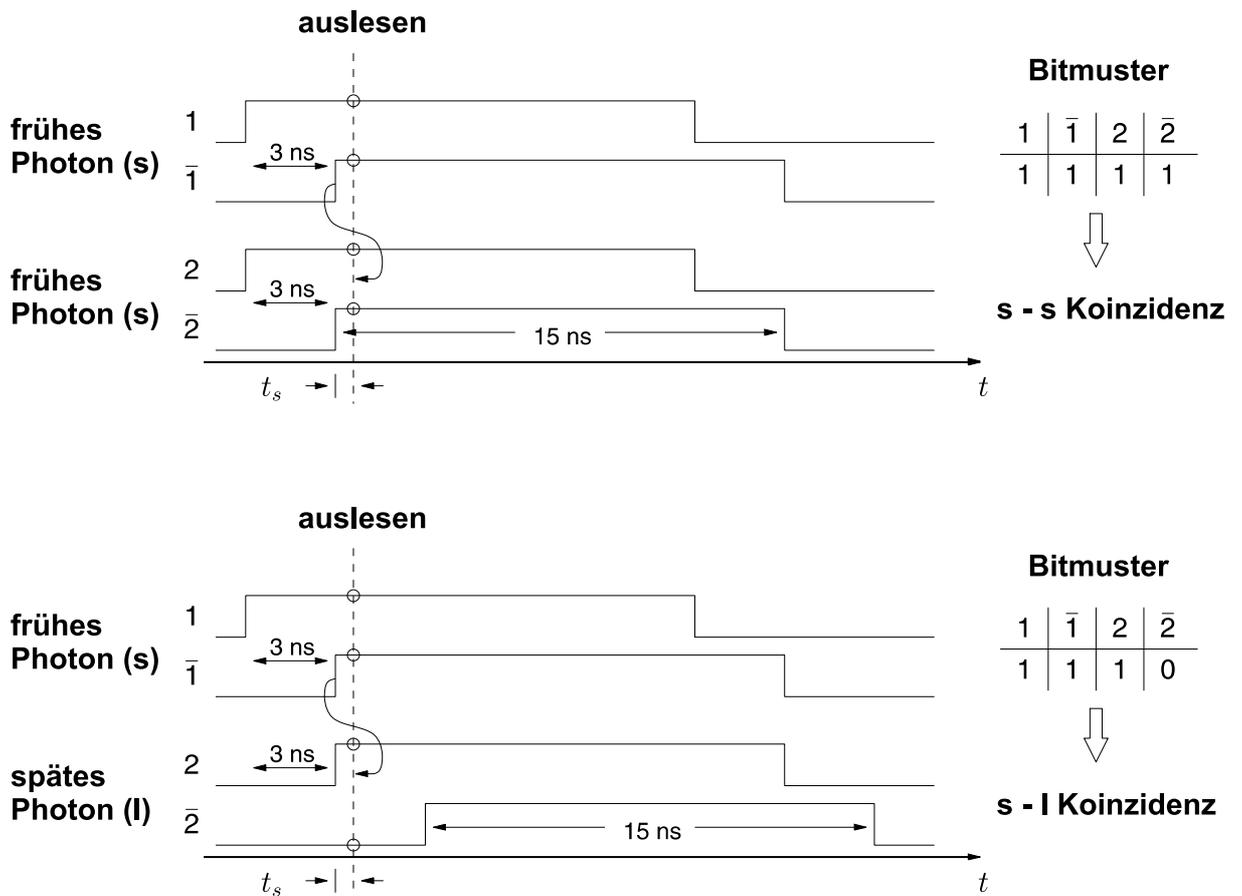


Abbildung 5.14: Zur Unterscheidung der frühen und späten Ereignisse durch die Koinzidenzeinheit.

Wie man in Abb. 5.9 sehen kann, ist die zeitliche Verteilungen der Detektorsignale recht breit (0.8 ns). Das bedeutet, dass die Detektorsignale von ($s - s$) Ereignissen nicht wirklich gleichzeitig am Register der Koinzidenzeinheit anliegen.

Dementsprechend kommen Detektorsignale von ($s - l$) Ereignissen nicht immer genau mit einer Verzögerung von $\Delta t = 3$ ns an den Registern der Koinzidenzeinheit an.

Deswegen war es notwendig, die Ausleseverzögerung t_s sehr exakt auf $\Delta t/2$ einzustellen. Ist t_s kleiner, so werden mehr gleichzeitige Ereignisse als ($s - l$) Ereignisse klassifiziert. Ist t_s größer als $\Delta t/2$, so werden mehr ($s - l$) Ereignisse für gleichzeitig gehalten.

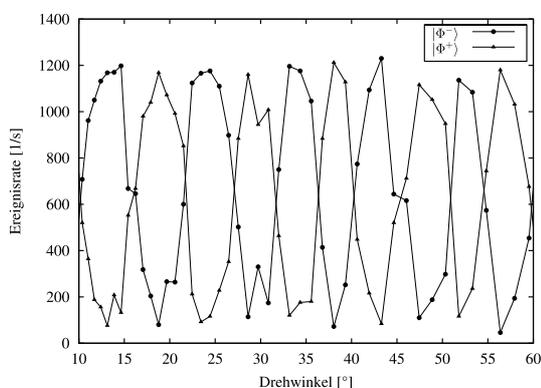
Um t_s einzustellen, habe ich das Signal einer Diode im fanout kopiert und an die Koinzidenzeinheit geschickt, wobei eines durch ein längeres Kabel um genau $\Delta t/2 = 1.5$ ns verzögert wurde. Verändert man nun t_s , so kann man beobachten, dass die Erkennung der zwei Signale an einer bestimmten Stelle zwischen "gleichzeitig" und "verzögert" umspringt. Dieser Wert für t_s wurde dann beibehalten. Eine Zeitdifferenz kleiner 1.5 ns

wird damit als "gleichzeitig" klassifiziert, eine größere als "verzögert".

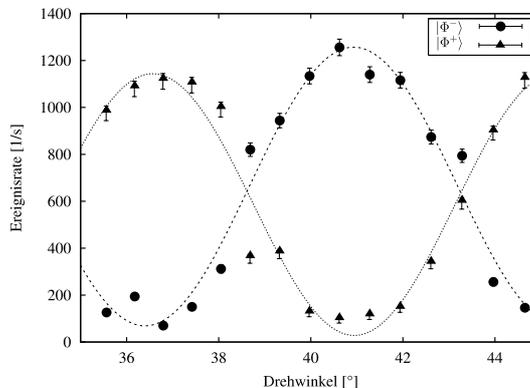
5.6 Ergebnisse

Bevor das Dense-Coding Protokoll durchgeführt werden kann, musste die relative Phase im asymmetrischen Interferometer so eingestellt werden, dass die Zustände $|\Phi^+\rangle$ und $|\Phi^-\rangle$ unterschieden werden können (vgl. Kap. 5.5.2).

Dazu wurde der Zustand $|\Phi^+\rangle$ vor dem ersten Strahlteiler eingestellt, und durch Drehung der Glasplatte im Stabilisierungsstrahl des langen Interferometerarms die relative Phase geändert. Dabei wurden alle Detektorsignaturen aufgenommen.



(a) Rate der $|\Phi^+\rangle$ - und $|\Phi^-\rangle$ -Ereignisse in Abhängigkeit vom Drehwinkel der Glasplatte. Die Linien verbinden die Datenpunkte. Pro Punkt wurde 2 s gemessen



(b) Vergrößerter Ausschnitt. Die Balken geben den statistischen Fehler an; die realen Fehler sind größer, da das Interferometer nicht absolut stabil ist. Die Kurven sind an die Daten angepasst.

Abbildung 5.15: Änderung der relativen Phase im asymmetrischen Interferometer.

Abb. 5.15(a) zeigt die Detektorsignaturen für die Zustände $|\Phi^+\rangle$ und $|\Phi^-\rangle$ während der Drehung der Glasplatte¹⁹. In Abb. 5.15(b) sieht man einen vergrößerten Ausschnitt, in dem eine Sinusfunktion an die Daten angepasst wurde. Man erkennt die erwarteten gegenläufigen Oszillationen mit Kontrasten von etwa 92%.

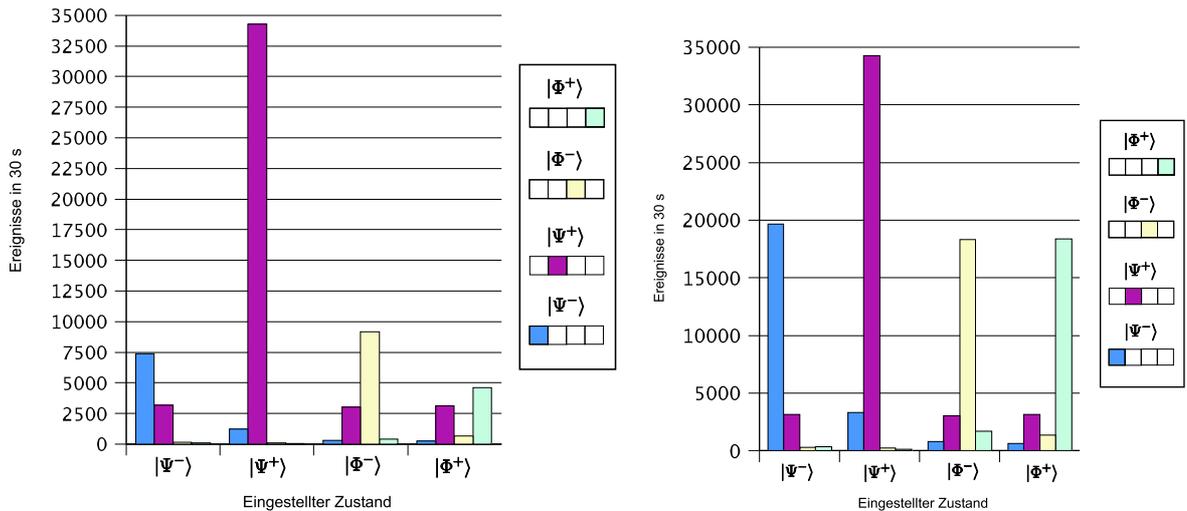
Dieser relativ geringe Wert ist wohl nicht in erster Linie auf eine schlechte Justage des Interferometers zurückzuführen, sondern darauf, dass die Stabilisierung des Interferometers zu schnelle Störungen wegen der Trägheit der Prismenmontierung nicht mehr ausgleichen kann.

¹⁹Daten sind auf Detektionswahrscheinlichkeiten korrigiert, siehe unten.

Nun wurden nacheinander alle vier Bell-Zustände durch Drehen der Wellenplättchen in Alices Arm 1 eingestellt (vgl. Kap. 4.5.2). Für jeden eingestellten Bell-Zustand wurden 30 Sekunden lang alle Detektorsignaturen aufgenommen.

Abb. 5.16(a) zeigt das Ergebnis einer solchen Messung.

In dieser Darstellung ist die gemessene Anzahl der zu den vier Bell-Zuständen gehörigen Detektorereignisse für alle vier Einstellungen in Alices Arm zu sehen.



(a) Unkorrigierte Zählraten für die Bellzustände (siehe Text).

(b) Zählraten für die Bellzustände, dividiert durch die theoretischen Detektionswahrscheinlichkeiten (siehe Text).

Abbildung 5.16: Zählraten der Zustandsanalyse in 30 s.

Dabei muss man beachten, dass die einzelnen Zustände wegen des Aufbaus nicht alle mit jeweils 100% Wahrscheinlichkeit detektiert werden können:

Die Detektionswahrscheinlichkeit für den Zustand $|\Psi^+\rangle$ ist gleich eins, da bei ihm jedes einzelne Photon in einer Diode nachgewiesen werden kann (vgl. Abb. 5.8 und Gl. 5.12, 5.13): $p_{\Psi^+} = 1$.

Für alle anderen Zustände ergibt sich ein Faktor $\frac{1}{2}$ in der Detektionswahrscheinlichkeit dadurch, dass bei der HOM-Interferenz beide Photonen zu D1 gehen können und dann nicht als Zweiphotonenereignis erkannt werden. Diesen Faktor $\frac{1}{2}$ könnte man umgehen, indem man in beiden Ausgängen des ersten Strahlteilers die komplette Analyse durchführt – und nicht nur in einem, wie es hier geschehen ist. Der Aufwand in der Koinzidenzanalyse würde jedoch stark anwachsen, da man dann in beiden Armen je vier Detektoren mit jeweils früh-spät Ereignissen benötigen würde.

Für den Zustand $|\Phi^-\rangle$ werden beide Photonen *nach* der HOM-Interferenz sicher detektiert (unterschiedliche PBS-Ausgänge im Detektormodul wegen Antikorrelation). Also ist $p_{\Phi^-} = \frac{1}{2} \cdot 1 = 0.5$.

Die zwei Photonen des Eingangszustandes $|\Phi^+\rangle$ werden an den Detektoren D2-D5 nur mit einer Wahrscheinlichkeit von 50% detektiert. Sie teilen sich nämlich am Detektormodul-PBS nicht auf und können nur als Koinziden gemessen werden, wenn sie sich am darauf folgenden Strahlteiler aufteilen. Dies geschieht mit 50% Wahrscheinlichkeit. In der anderen Hälfte der Fälle teilen sich die beiden Photonen am letzten Strahlteiler nicht auf und landen in *einem* der Detektoren D2-D5. Damit ist $p_{\Phi^+} = \frac{1}{2} \cdot \frac{1}{2} = 0.25$.

Der Eingangszustand $|\Psi^-\rangle$ resultiert hinter dem polarisierenden Strahlteiler im Detektormodul in der Hälfte der Fälle in zwei Photonen in verschiedenen Strahlteilermoden (Amplituden $|HV\rangle, |VH\rangle$). Dann wird er mit Sicherheit detektiert. In der anderen Hälfte der Fälle (Amplituden $|HH\rangle, |VV\rangle$) erhält die Detektionswahrscheinlichkeit noch einen Faktor $\frac{1}{2}$, weil sich die Photonen am letzten Strahlteiler nur mit 50% Wahrscheinlichkeit aufteilen. Damit ergibt sich $p_{\Psi^-} = \frac{1}{2} \cdot \frac{1}{2}(1 + \frac{1}{2}) = 0.375$.

In Abb. 5.16(b) wurden die Zählraten der einzelnen Zustände mit ihrer inversen (theoretischen) Detektionswahrscheinlichkeit ($p_{\Psi^\pm}, p_{\Phi^\pm}$) multipliziert, um die Ereignisraten besser vergleichen zu können.

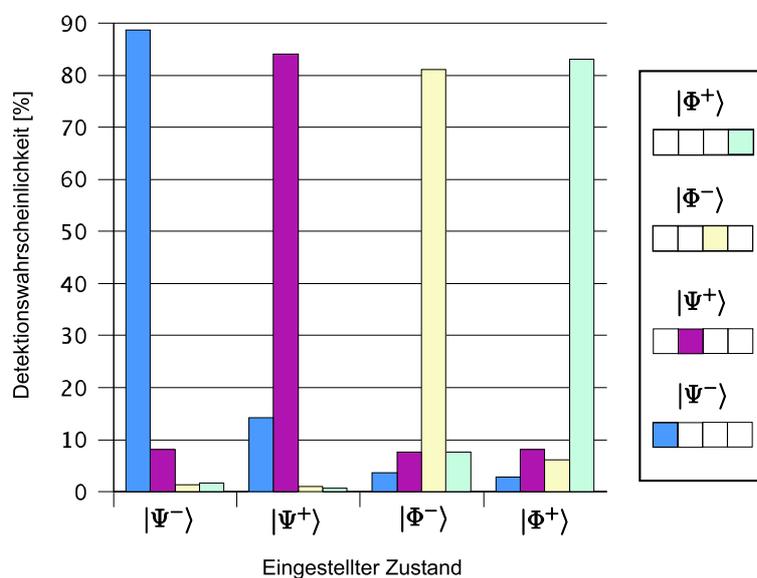


Abbildung 5.17: Detektionswahrscheinlichkeiten der vier Bellzustände, korrigiert auf Detektionswahrscheinlichkeit und unterschiedliche Kopplungseffizienz (siehe Text).

Man muss bei der Interpretation der Daten in Abb. 5.16(b) außerdem bedenken, dass die Photonen – vom ersten Strahlteiler der HOM-Interferenz kommend – unterschiedlich stark an den Detektor D1 beziehungsweise die Detektoren D2-D5 koppeln. Das liegt hauptsächlich an Verlusten auf dem Weg durch das Interferometer, und die optischen Elemente der Polarisationsanalyse, die auf dem Weg zu D1 nicht auftreten. Eine zum ersten Strahlteiler "symmetrische" Analyse würde auch dies ausgleichen.

In Abb. 5.17 wurden die Zählraten der Detektoren D2-D5 daher auf die Kopplungseffizienz zu D1 normiert dargestellt. Es sind die bedingten Wahrscheinlichkeiten zu sehen, dass ein Bell-Zustand erkannt wird, wenn ein anderer (oder natürlich der gleiche) Bell-Zustand präpariert worden ist. Man kann an Abb. 5.17 erkennen, dass die Wahrscheinlichkeit einer korrekten Klassifizierung jedes einzelnen Bell-Zustands bei etwa 80% bis 88% liegt²⁰.

Der (fast konstante) Hintergrund an $|\Psi^+\rangle$ -Ereignissen bei den anderen drei Zuständen ist recht hoch. Dies liegt an dem etwas geringeren Dip-Kontrast, der bei dieser Messung erreicht wurde. Er betrug leider nur zwischen 86% und 90% für die "dips" (siehe Abb. 5.18).

Das erklärt auch den Hintergrund an $|\Psi^-\rangle$ -Ereignissen, als $|\Psi^+\rangle$ eingestellt war. Wenn sich der Eingangszustand $|\Psi^+\rangle$ wegen unperfekter Justage am Strahlteiler nicht aufteilt, wird er aufgrund seiner Polarisationsantikorrelation als $|\Psi^-\rangle$ klassifiziert. Der geringe Prozentsatz der Fälle, in denen ein $|\Psi\rangle$ -Zustand als $|\Phi\rangle$ -Zustand klassifiziert wird, kommt wahrscheinlich von der nicht ganz 100%igen Zustandspräparation.

Der $|\Psi^-\rangle$ -Anteil bei den Zuständen $|\Phi^\pm\rangle$ ist hauptsächlich der breiten Verteilung der Detektormodul-Ausgangssignale zuzurechnen. Deswegen werden $s - l$ -Ereignisse detektiert, obwohl die Zustände den gleichen Weg zurücklegten.

Die nicht perfekte Stabilität des Interferometers äußert sich in einem Hintergrund an $|\Phi^-\rangle$ beim Zustand $|\Phi^+\rangle$ und umgekehrt.

Ich komme also zu dem Schluss, dass die vier Bell-Zustände mit dem hier vorgestellten Verfahren mit hohen Wahrscheinlichkeiten unterschieden werden können. Außerdem sind die Gründe der falschen Klassifizierungen weitgehend klar.

Einer der ersten Schritte zur Reduktion dieser falschen Klassifizierungen müsste die Verbesserung des Kontrasts der HOM-Interferenz sein. So würde der $|\Psi^+\rangle$ -Hintergrund bei den Zuständen verringert²¹. Dass höhere "dip"-Kontraste experimentell möglich sind, wurde in Kap. 5.5.1 gezeigt.

Eine weitere Verbesserung der Resultate würde mit Sicherheit eine größere zeitliche Trennung der $(s - l)$ -Ereignisse mit sich bringen. Auf diese Weise würde der $|\Psi^-\rangle$ -

²⁰Die Werte sind in Tabelle 5.2 angegeben.

²¹bzw. der $|\Psi^-\rangle$ -Hintergrund beim Zustand $|\Psi^+\rangle$ selbst, s.o.

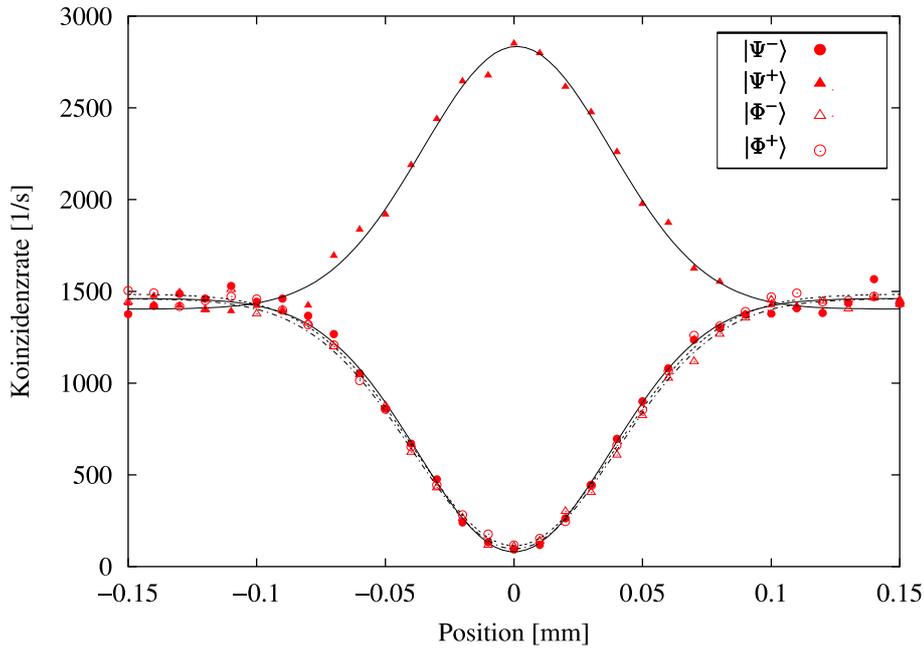


Abbildung 5.18: Koinzidenzraten bei der HOM-Interferenz; vgl. Abb. 5.6.

Hintergrund reduziert werden.

Die Detektionswahrscheinlichkeiten in Abb. 5.17 entsprechen der in Tabelle 5.2 angegebenen Transfermatrix des Kanals im Dense Coding-Protokoll.

Angegeben sind die bedingten Wahrscheinlichkeiten $p(y|x)$, dass das "Symbol" $Y \in \{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$ von Bob erkannt wurde, wenn $X \in \{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$ von Alice gesendet wurde.

$X \setminus Y$	$ \Psi^-\rangle$	$ \Psi^+\rangle$	$ \Phi^-\rangle$	$ \Phi^+\rangle$
$ \Psi^-\rangle$	88.8	8.2	1.4	1.7
$ \Psi^+\rangle$	14.3	84.0	1.1	0.7
$ \Phi^-\rangle$	3.6	7.6	81.1	7.6
$ \Phi^+\rangle$	2.9	8.1	6.1	83.0

Tabelle 5.2: Transfermatrix des Kanals.

Nach Gl. 2.7 kann daraus die gegenseitige Information von Alice und Bob (bei Gleichverteilung von X) zu $I(X : Y) = 1.18$ bit berechnet werden. Der relative Fehler dieser Messung liegt wegen niedriger Zählraten bei etwa 10%.

Ich möchte noch darauf hinweisen, dass die Kapazität des Kanals (Gl. 2.13) noch höher ist, da das Rauschen des Kanals nicht isotrop verteilt ist. Die gegenseitige Information kann also durch geeignete Kodierung der Quelle noch erhöht werden.

6 Zusammenfassung und Ausblick

In der vorliegenden Arbeit konnte ich die deterministische und vollständige Bell-Zustandsanalyse an polarisationskodierten Photonen mit passiven, linearoptischen Elementen präsentieren. Die Analyse macht dabei keinen Gebrauch von Hilfsphotonen oder bedingter Dynamik.

Die Unterscheidung aller vier maximal verschränkten Zustände wurde erreicht, indem die Verschränkung der Photonenpaare in weiteren Freiheitsgraden – der Energie bzw. Zeit – ausgenutzt wurde. Diese zusätzliche Verschränkung resultiert, wie die Polarisationsverschränkung, aus dem Erzeugungsprozess der Photonenpaare, der spontanen parametrischen Fluoreszenz vom Typ II.

Die vier Bell-Zustände werden mit Wahrscheinlichkeiten zwischen 81% und 89% korrekt identifiziert. Außerdem konnte gezeigt werden, an welcher Stelle die Analyse von experimentellen Imperfektionen am stärksten beeinträchtigt wird, und wie diese größtenteils in den Griff zu bekommen sind.

Durch die vollständige Bell-Zustandsanalyse konnte ich optimales superdichtes Quantenkodieren implementieren, bei dem erstmals durch die Unterscheidung aller vier Bell-Zustände gezeigt werden konnte, dass die klassische Kanalkapazität von einem bit durch das Quantenkodieren übertroffen wird. Die lokalen Operationen von Alice wurden durch eine einfache Kombination von Wellenplättchen, die die Polarisation des Bell-Zustands manipulieren, durchgeführt.

Die vollständige Bell-Zustandsanalyse kann dazu verwendet werden, Protokolle wie das superdichte Quantenkodieren effizienter durchzuführen. Mit dem hier verwendeten Aufbau wäre es jedoch auch möglich, zum Beispiel so genannte Quantenspiele [61] durchzuführen. Im Gegensatz zum superdichten Quantenkodieren dürfen in den Protokollen der Quantenspiele beide Parteien, Alice und Bob, ihre Qubits manipulieren. Danach werden sie in Abhängigkeit des Zustands, den sie erzeugt haben, entlohnt. Diesen Zustand könnten wir jetzt durch die vollständige Analyse bestimmen. Die Messung aller vier Bell-Zustände ist in diesem Fall absolut notwendig.

Während uns die zeitlichen Korrelationen der Photonenpaare die vollständige Bell-Zustandsanalyse einerseits erst ermöglichen, schränken sie ihre Universalität andererseits dementsprechend ein. Eine vollständige Bell-Projektion an Photonenpaaren, die

diese zeitlichen Korrelationen nicht aufweisen, die also nicht Energie-Zeit-verschränkt sind, ist daher nicht möglich. Deswegen kann man zum Beispiel bei der Durchführung des Teleportationsprotokolls [2] nicht von dem hier vorgestellten Verfahren profitieren, da die zwei Photonen, die auf die Bell-Basis projiziert werden müssen, in keinem Freiheitsgrad verschränkt oder korreliert sind.

Damit ist die Wirkung unserer besonderen Bell-Projektion auch nicht mit der eines universellen CNOT-Gatters gleichzusetzen, das aus zwei vollkommen unkorrelierten Qubits maximal verschränkte Zustände generieren kann und umgekehrt. Im Besonderen scheint die Verwendung in Gatter-Netzwerken nicht praktikabel, da hier wiederum a priori gänzlich unkorrelierte Photonen prozessiert werden müssten. Zu diesem Zweck scheinen andere Verfahren geeigneter zu sein.

GASPARONI ET AL. konnten ein optisches CNOT-Gatter realisieren, das für den Einsatz in einem Gatter-Netzwerk geeignet zu sein scheint [50]. Es greift nur auf lineare optische Mittel zurück und verwendet zwei zusätzliche, verschränkte Hilfsphotonen. Es hat den Vorteil, dass man durch Messungen in bestimmten Moden an den Hilfsphotonen (also nicht am control- oder target-Qubit) feststellen kann, ob die CNOT-Operation erfolgreich war oder nicht. Diese Information kann dann an die darauf folgenden Elemente weitergegeben werden.

Ein weiterer interessanter Ansatz stammt von RAUSSENDORF und BRIEGEL [62], das Konzept der so genannten "cluster"-Zustände. Die Berechnung erfolgt hier nicht in einem Netzwerk von Quantengattern. Vielmehr dient der cluster-Zustand, der aus vielen verschränkten Qubits besteht, als "Einweg-Computer", an dem das "Programm" der Berechnung erst durch Messungen an ihm festgelegt wird. Die Messungen werden am einzelnen Qubit durchgeführt [62]. Obwohl die Zustände ursprünglich für Systeme mit Ising-ähnlicher Spin-Spin Wechselwirkung vorgesehen waren, sind auch optische Realisierungen möglich.

Wenn man die Entwicklungen in der Quanteninformatik und -kommunikation beobachtet, scheint es zwar noch ein weiter Weg bis zum praktischen Einsatz eines Quantencomputers zu sein, aber *dass* er früher oder später realisierbar sein wird, lässt sich schwer bezweifeln.

Davon abgesehen wird es sicher ein sehr spannender Prozess sein, weiter zu verstehen, wie fundamental die Rolle der Information in der Physik tatsächlich ist.

A Anhang

A.1 Fit-Funktionen und Kontrast

Unter dem Kontrast (engl. "visibility") V einer Funktion mit Maximalwert M und Minimalwert m verstehe ich im Allgemeinen das Verhältnis $V = \frac{M-m}{M+m}$.

Bei sinusförmigem Verlauf der Funktion wird die Funktion

$$f_{\sin}(x) := \frac{A}{2} (1 - V \sin 2(x - x_0)) \quad (\text{A.1})$$

verwendet. A ist die doppelte Amplitude der Oszillation mit perfektem Kontrast ($|V| = 1$). Es ist $f_{\sin}(x = x_0) = \frac{A}{2}$.

Gaußförmige Abhängigkeiten werden via

$$f_{\text{Gauß}}(x) := y_0 \left(1 + \frac{2V}{1-V} \exp \left(-\frac{(x - x_0)^2}{2\sigma^2} \right) \right) \quad (\text{A.2})$$

modelliert. Dabei nimmt die Funktion für $x \rightarrow \pm\infty$ den Wert y_0 an. $|V|$ ist der Kontrast, x_0 die Position des Maximums und σ die Standardabweichung.

Es ist $\text{FWHM} = 2\sqrt{2 \ln 2} \cdot \sigma \approx 2.35 \cdot \sigma$.

A.2 Wellenplättchen-Matrizen

Verwende für die Darstellungen der Wirkung eines Halb- bzw. Viertelwellenplättchens in der Standardbasis die Matrizen

$$U_{\lambda/2}(\alpha) \doteq \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}, \quad (\text{A.3})$$

$$U_{\lambda/4}(\beta) \doteq \begin{pmatrix} \cos^2 \beta - i \sin^2 \beta & \frac{1}{2}(1+i) \sin 2\beta \\ \frac{1}{2}(1+i) \sin 2\beta & \sin^2 \beta - i \cos^2 \beta \end{pmatrix} \quad (\text{A.4})$$

wo α bzw. β der Winkel zwischen optischer Achse und der Senkrechten ist.

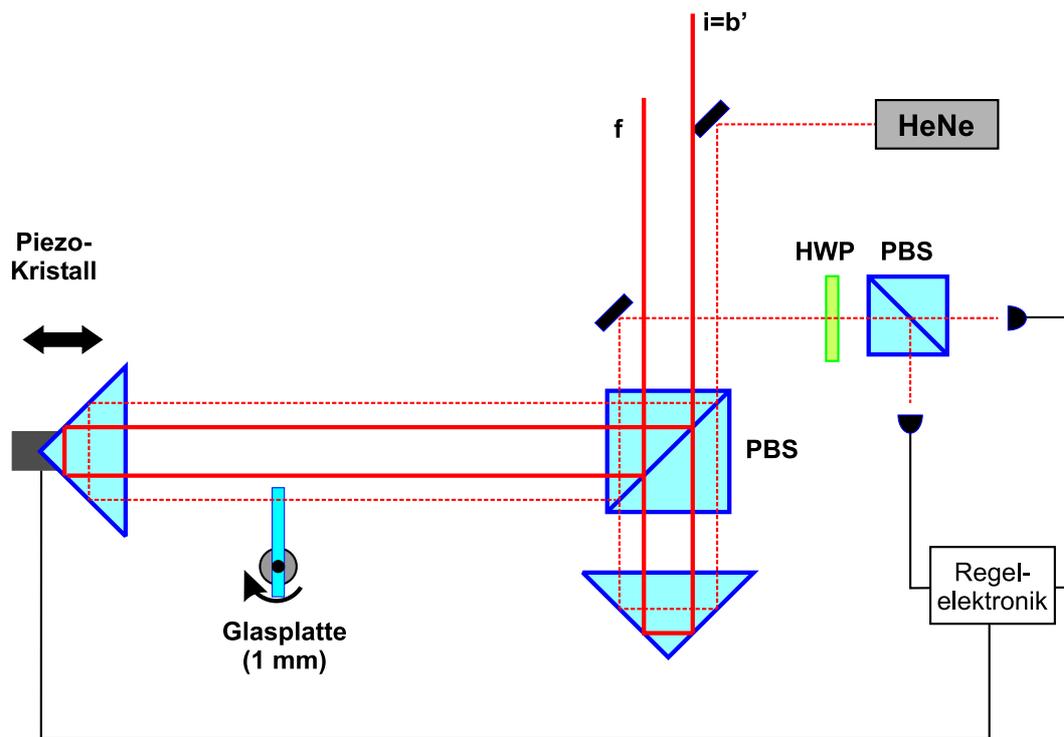


Abbildung A.1: Das asymmetrische Interferometer mit Stabilisierungsaufbau.

A.3 Stabilisierung des Interferometers

Wie man Gl. 5.7 entnehmen kann, ist die Stabilität der relativen Phase 2γ im Interferometer für die Unterscheidung der Zustände $|\Phi^-\rangle$ und $|\Phi^+\rangle$ essentiell. Ändert sich der Längenunterschied der zwei Interferometerarme um eine Wellenlänge (entspricht Phasenanschub $2\gamma = 2\pi$), so würde plötzlich ein $|\Phi^-\rangle$ als $|\Phi^+\rangle$ identifiziert werden und umgekehrt¹. Das Interferometer musste aktiv stabilisiert werden, da schon geringe Luftbewegungen erheblichen Einfluss auf γ haben.

Der Aufbau zur Stabilisierung des Interferometers ist in Abb. 5.7 zu sehen. Etwa 1 cm unter dem Verlauf der Einzelphotonen wird der Strahl eines HeNe-Lasers² auf dem sonst gleichen Weg durch das gesamte Interferometer geschickt.

Durch ein Halbwellenplättchen auf 22.5° wird die "welcher-Weg-Information", die am Interferometer-PBS in der Polarisierung kodiert wurde, für den zweiten polarisierenden Strahlteiler wieder gelöscht, sodass die Amplituden aus dem langen und dem kurzen Arm interferieren können.

Die Lichtintensität in einer Ausgangsmode dieses Strahlteilers ist somit abhängig von

¹Der durch das Interferometer verursachte *globale* Phasenfaktor bei $|\Psi^-\rangle$ spielt keine Rolle.

² $\lambda = 632.8 \text{ nm}$; Die Kohärenzlänge ist wesentlich größer als der Wegunterschied im Interferometer.

der relativen Phase, die die H- und V-Amplituden durch das Interferometer erhalten. Die Intensitäten in beiden Ausgangsmoden des PBS sind in ihrer Abhängigkeit dieser Phase genau um π versetzt.

Die Lichtintensitäten in den PBS-Ausgangsmoden wurden mit Standard PIN-Photodioden gemessen. Aus deren Photostrom wurde in der Stabilisierungselektronik ein Fehlersignal erzeugt, das nach Hochspannungsverstärkung als Regelsignal für einen Piezokristall benutzt werden kann.

Dieser Piezokristall reguliert die Länge des langen Interferometerarms und somit die relative Phase zwischen den Armen, indem er das Prisma bewegt. Damit ist der Regelkreis geschlossen. Wegen der Trägheit der Prismenmontierung sind nur Störungen langsamer als etwa 1 Hz kompensierbar.

Es stellte sich heraus, dass die Interferometerphase 2γ extrem empfindlich auf Vibrationen der optischen Elemente sowie Luftbewegungen ist. Letztere verursachen geringe Änderungen des Brechungsindex der Luft im Interferometer; sie können mit der aktiven Stabilisierung gut ausgeglichen werden.

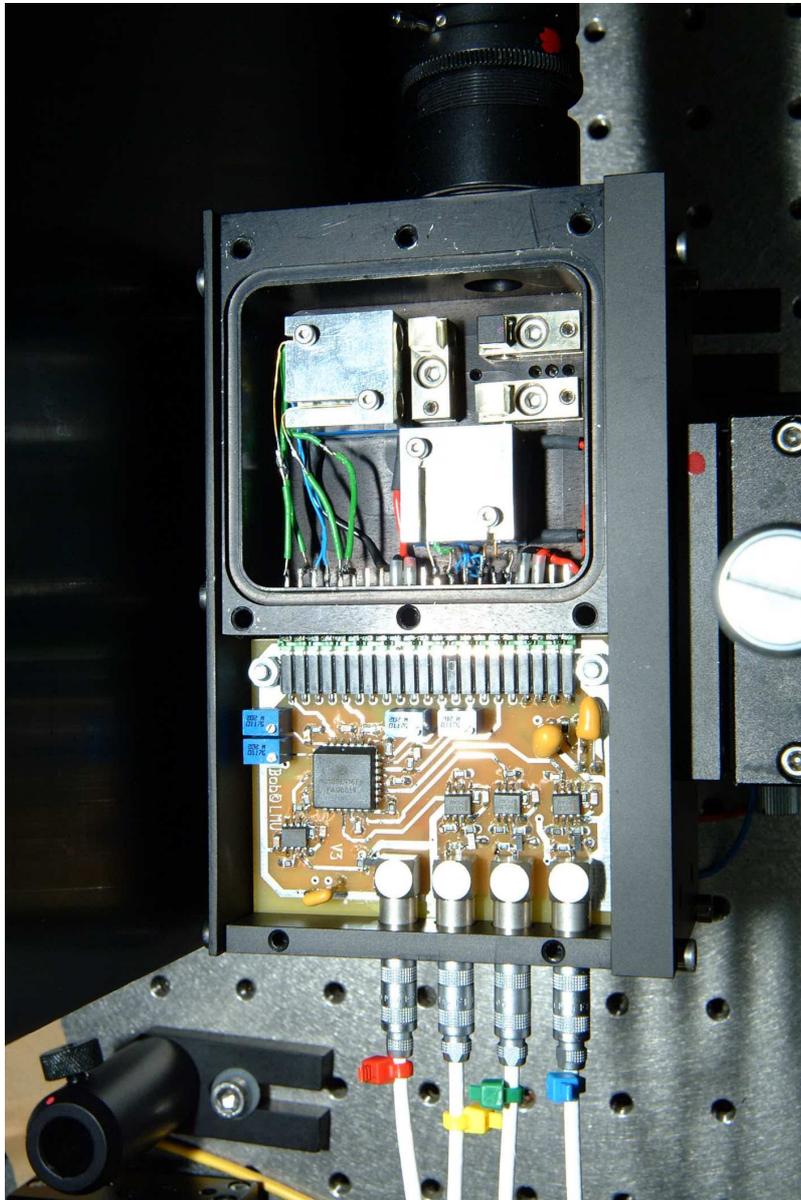
Wahrscheinlich verursachte der Ventilator unseres elektronischen Detektionsmoduls die größten Störungen, sowohl durch Vibration als auch durch die Luftbewegung.

Um die relative Phase 2γ im Interferometer nicht nur konstant zu halten (das erreicht die Stabilisierung), sondern auf genau den Wert einzustellen, der es uns ermöglicht, $|\Phi^+\rangle$ und $|\Phi^-\rangle$ zu unterscheiden, läuft der Strahl des HeNe-Lasers im langen Interferometerarm durch eine 1 mm dicke Glasplatte.

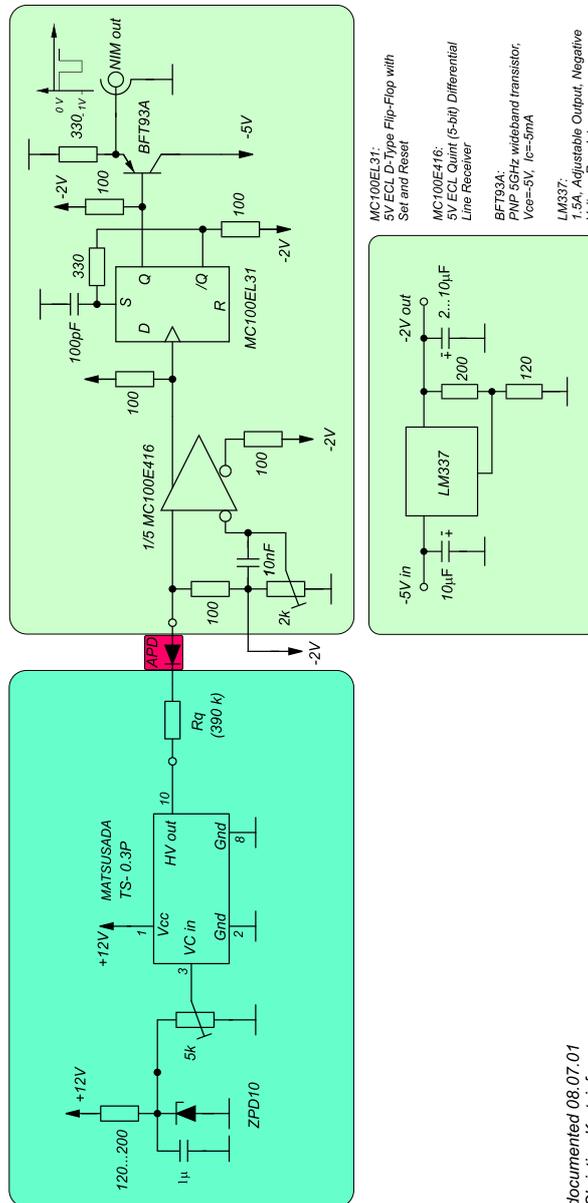
Wenn diese gedreht wird, ändert sich die relative Phase der Stabilisierungsstrahlen, was die Kontrollelektronik dadurch kompensiert, dass sie den Arm länger oder kürzer macht. Dadurch ändert sich der Wegunterschied für die Einzelphotonen, die *über* der Glasplatte verlaufen.

Auf diese Weise kann also der relative Phasenfaktor $e^{i2\gamma}$ durch Drehen der Glasplatte durchgeführt werden. Die richtige Position kann dadurch gefunden werden, dass man den Zustand $|\Phi^+\rangle$ einstellt und in Abhängigkeit vom Drehwinkel der Glasplatte die Detektorsignaturen für die verschiedenen Bell-Zustände beobachtet.

A.4 Die Detektoreinheit



bob circuit



documented 08.07.01
Christian Kurtsiefer

Abbildung A.2: Der Schaltplan der Detektoreinheit

Literaturverzeichnis

- [1] A. Einstein, B. Podolski und N. Rosen.
Can quantum-mechanical description of physical reality be considered complete?
Phys. Rev., **47**:777–780, (1935).
- [2] C. H. Bennett et al.
Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.
Phys. Rev. Lett., **70**:1895, (1993).
- [3] C. H. Bennett und S. J. Wiesner.
Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states.
Phys. Rev. Lett., **69**:2881, (1992).
- [4] J. Calsamiglia und N. Lütkenhaus.
Maximum efficiency of a linear-optical Bell-state analyzer.
Appl. Phys. B, **72**:67–71, (2001).
- [5] P. G. Kwiat und H. Weinfurter.
Embedded Bell-state analysis.
Phys. Rev. A, **58**:R2623, (1998).
- [6] C. E. Shannon.
A mathematical theory of communication.
Bell System Technical Journal, **27**:379–423, 623–656, (1948).
- [7] M. A. Nielsen und I. L. Chuang.
Quantum computation and quantum information.
Cambridge; University Press, (2002).
- [8] T. M. Cover und J. A. Thomas.
Elements of Information Theory.
John Wiley and Sons, (1991).

- [9] C. Kurtsiefer et al.
A step towards global key distribution.
Nature, **419**:450, (2002).
- [10] B. Schumacher.
Quantum coding.
Phys. Rev. A, **51**:2738, (1993).
- [11] W. K. Wootters und W. H. Zurek.
A single quantum cannot be cloned.
Nature, **299**:802, (1982).
- [12] A. S. Holevo.
Some estimates for information quantity transmitted by quantum communication.
Probl. Inform. Transm., **9**:177, (1973).
- [13] C. H. Bennett und G. Brassard.
Quantum cryptography: public key distribution and coin tossing.
Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (1984).
- [14] E. Schrödinger.
Discussion of probability relations between separated systems.
Proceedings of the Cambridge Philosophical Society, **31**:555, (1935).
- [15] H. P. H. R. Horodecki, M.
Separability of mixed states: necessary and sufficient conditions.
Phys. Lett. A, **223**:1, (1996).
- [16] P. Horodecki.
Separability criterion and inseparable mixed states with positive partial transposition.
Phys. Lett. A, **232**:333, (1997).
- [17] C. A. Sacket et al.
Experimental entanglement of four particles.
Nature, **404**:256, (2000).
- [18] J.-W. Pan et al.
Experimental demonstration of four-photon entanglement and high-fidelity teleportation.
Phys. Rev. Lett., **86**:4435, (2001).

- [19] Z. Zhao et al.
Experimental demonstration of five-photon entanglement and open-destination teleportation.
 Nature, **430**:54, (2004).
- [20] J. S. Bell.
On the Einstein-Podolsky-Rosen Paradox.
 Physics, **1**:195–200, (1964).
- [21] S. J. Freedman und J. F. Clauser.
Experimental test of local hidden-variable theories.
 Phys. Rev. Lett., **28**:938, (1972).
- [22] A. Aspect, J. Dalibard und G. Roger.
Experimental test of Bell's inequalities using time-varying analyzers.
 Phys. Rev. Lett., **49**:1804, (1982).
- [23] A. Aspect, J. Grangier, Philippe und G. Roger.
Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of bell's inequalities.
 Phys. Rev. Lett., **49**:91, (1982).
- [24] J. F. Clauser, M. Horne, A. Shimony und R. Holt.
Proposed experiment to test local hidden-variable theories.
 Phys. Rev. Lett., **23**:880, (1969).
- [25] 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, (1998).
- [26] M. A. Rowe.
Experimental violation of a Bell's inequality with efficient detection.
 Nature, **409**:7910, (2001).
- [27] B. Blinov, D. Moehring, L.-M. Duan und C. Monroe.
Observation of entanglement between a single trapped atom and a single photon.
 Nature, **428**:153, (2004).
- [28] W. Tittel, J. Brendel, H. Zbinden und N. Gisin.
Violation of Bell inequalities by photons more than 10 km apart.
 Phys. Rev. Lett., **81**:3563, (1998).
- [29] H.-K. Lo, S. Popescu und T. Spiller.
Introduction to quantum computation and information.
 World Scientific, (1998).

- [30] D. A. Kleinman.
Theory of optical parametric noise.
Phys. Rev., **174**:1027, (1968).
- [31] B. R. Mollow.
Photon correlations in the parametric frequency splitting of light.
Phys. Rev. A, **8**:2684, (1973).
- [32] C. K. Hong und L. Mandel.
Theory of parametric frequency downconversion of light.
Phys. Rev. A, **31**:2409, (1985).
- [33] M. Oberparleiter.
Effiziente Erzeugung verschränkter Photonenpaare.
Dissertation, (2002).
- [34] P. G. Kwiat, K. Mattle, H. Weinfurter und A. Zeilinger.
New High-Intensity Source of Polarization-Entangled Photon Pairs.
Phys. Rev. Lett., **75**:4337, (1995).
- [35] C. Kurtsiefer, M. Oberparleiter und H. Weinfurter.
High-efficiency entangled photon pair collection in type-II parametric fluorescence.
Phys. Rev. A, **64**:023802, (2001).
- [36] C. Schuck.
Experimental implementation of a quantum game.
Diplomarbeit, (2003).
- [37] D. Bouwmeester et al.
Experimental Quantum Teleportation.
Nature, **390**:575, (1997).
- [38] J.-W. Pan, D. Bouwmeester, H. Weinfurter und A. Zeilinger.
Experimental Entanglement Swapping: Entangling Photons That Never Interacted.
Phys. Rev. Lett., **80**:3891, (1998).
- [39] T. Jennewein, G. Weihs, J.-W. Pan und A. Zeilinger.
Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping.
Phys. Rev. Lett., **88**:017903, (2002).

- [40] H.-J. Briegel, W. Dür und J. Cirac.
Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication.
Phys. Rev. Lett., **81**:5932, (1998).
- [41] A. Poppe et al.
Practical quantum key distribution with polarization entangled photons.
quant-ph/0404115, (2004).
- [42] P. van Loock und N. Lütkenhaus.
Simple criteria for projective measurements with linear optics.
quant-ph/0304057, (2003).
- [43] E. Knill, R. Laflamme und G. J. Milburn.
Efficient linear optics quantum computation.
quant-ph/0006088, (2000).
- [44] S. Gosh et al.
Distinguishability of Bell States.
Phys. Rev. Lett., **87**:277902, (2001).
- [45] K. Mattle, H. Weinfurter, P. Kwiat und A. Zeilinger.
Dense Coding in Experimental Quantum Communication.
Phys. Rev. Lett., **76**:4656, (1996).
- [46] S. L. Braunstein und A. Mann.
Measurement of the Bell operator and quantum teleportations.
Phys. Rev. A, **51**:R1727, (1995).
- [47] M. Michler, K. Mattle, H. Weinfurter und A. Zeilinger.
Interferometric Bell-state analysis.
Phys. Rev. A, **53**:R1209, (1996).
- [48] E. Knill, R. Laflamme und G. J. Milburn.
A scheme for efficient quantum computation with linear optics.
Nature, **409**:46, (2001).
- [49] Z. Zhao et al.
Experimental demonstration of a non-destructive controlled-NOT quantum gate for two independent photon-qubits.
quant-ph/0404129, (2004).
- [50] S. Gasparoni et al.
Realization of a photonic CNOT gate sufficient for quantum computation.
quant-ph/0404107, (2004).

- [51] J. L. O'Brien et al.
Demonstration of an all-optical quantum controlled-NOT gate.
Nature, **426**:264, (2003).
- [52] J. Franson.
Bell inequality for position and time.
Phys. Rev. Lett., **62**:2205, (1989).
- [53] P. G. Kwiat, W. A. Vareka, C. K. Hong, H. Nathel und R. Y. Chiao.
Correlated two-photon interference in a dual-beam Michelson interferometer.
Phys. Rev. A, **41**:2910, (1990).
- [54] P. G. Kwiat, A. M. Steinberg und R. Y. Chiao.
High-visibility interference in a Bell-inequality experiment for energy and time.
Phys. Rev. A, **47**:R2472, (1993).
- [55] V. Scarani, G. N. und S. Popescu.
Proposal for Energy-Time Entanglement of Quasiparticles in a Solid-State Device.
Phys. Rev. Lett., **92**:167901, (2004).
- [56] W. Tittel et al.
Quantum Cryptography Using Entangled Photons in Energy-Time Bell States.
Phys. Rev. Lett., **84**:4737, (2000).
- [57] C. Cinelli, M. Barbieri, F. De Martini und P. Mataloni.
Experimental realization of hyper-entangled two-photon states.
quant-ph/0406148, (2004).
- [58] C. K. Hong, Z. Y. Ou und L. Mandel.
Measurement of subpicosecond time intervals between two photons by interference.
Phys. Rev. Lett., **59**:2044, (1987).
- [59] T. B. Pittman et al.
Can Two-Photon Interference be Considered the Interference of Two Photons?
Phys. Rev. Lett., **77**:1917, (1996).
- [60] C. Kurtsiefer, P. Zarda, S. Mayer und H. Weinfurter.
The breakdown flash of silicon avalanche photodiodes-backdoor for eavesdropper attacks?
J. Mod. Opt., **48**:2039, (2001).

- [61] J. Eisert, M. Wilkens und M. Lewenstein.
Quantum games and quantum strategies.
Phys. Rev. Lett., **83**:3077, (1998).
- [62] R. Raussendorf und H. Briegel.
A one-way quantum computer.
Phys. Rev. Lett., **86**:5188, (2001).

Erklärung

Mit der Abgabe der Diplomarbeit erkläre ich, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

München, den 9. August 2004.

Gerhard Huber