Präparation von destillierten und purifizierten gequetschten Zuständen

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des Grades

Doktor der Naturwissenschaften
– Dr. rer. nat. –

genehmigte Dissertation
von

Dipl.-Phys. Alexander Franzen

geboren am 25. Mai 1977 in Würzburg

2008

Referent:	Juniorprof. Dr. Roman Schnabel
Korreferent:	Prof. Dr. K. Danzmann
Tag der Promotion:	31.01.2008

Für S & M & E

Inhaltsverzeichnis

Abbildungsverzeichnis

Abstract

The distillation and purification of nonclassical quantum states of light is one of the key requirements for optical quantum communication with the purpose to counteract decoherence and to regain the nonclassical properties of squeezed, entangled and Fock-states. The basic principle behind any distillation-protocol is, to extract from a high number of weakly nonclassical quantum states a lesser number of strongly nonclassical states, thus forming one of the building blocks of a „quantum repeater“. Continuous variable states are of particular interest, because important quantum information processing primitives could be implemented with only linear optics, optical parametric amplifiers and homodyne detection.

In this thesis the first experimental preparation of distilled and purified nonclassical states is presented.

We describe the theoretical investigation and experimental examination of a distillation protocol for squeezed states that only relies on linear optics and post-processing. Two copies of a squeezed state have been generated using optical parametric amplification. These states have been intentionally exposed to random phase noise which mimics the effect of a noisy optical transmission. Using these states, a complete distillation protocol has been experimentally realised. The distilled states are made available for further experiments, contrasting earlier experiments in the discrete variable („single photons“) regime, in which the distilled states are typically destroyed under application of the protocol, prohibiting any practical application. During the course of work the protocol revealed far greater complexity and possibilities than initially assumed. Three of those extensions, namely *conjugate distillation*, *quantum channel probing* and *phase randomized distillation* have been investigated.

Keywords: Quantum information, nonclassical light, distillation

Kurzfassung

Die Destillation und Purifikation von nichtklassischen Zuständen des Lichtes ist eine Grundvorraussetzung für optische Quantenkommunikation und verfolgt das Ziel, Effekte von Dekohärenz zu beseitigen und die nichtklassischen Eigenschaften von gequetschten, verschränkten und Fockzuständen, zurück zu gewinnen. Das Grundprinzip jedes Destillationsprotokolls besteht darin, aus einer großen Anzahl schwach nichtklassischer Zustände eine geringere Anzahl stark nichtklassischer Zustände zu extrahieren. Es stellt damit einen der Grundbausteine eines „Quanten-Repeaters“ dar. Kontinuierliche Variablen sind von besonderem Interesse, da wichtige Grundbausteine der Quanteninformationsverarbeitung allein mittels linearer Optik, optisch parametrischen Verstärkern und Homodyndetektion implementiert werden können.

In der vorliegenden Arbeit wird die erste experimentelle Präparation destillierter und purifizierter nichtklassischer Zustände präsentiert.

Wir beschreiben die theoretische Untersuchung und experimentelle Überprüfung eines Destillationsprotokolls für gequetschte Zustände, das lediglich auf linearer Optik und Nachbearbeitung basiert. Zwei Kopien eines gequetschten Zustandes wurden mittels optisch parametrischer Verstärkung erzeugt. Diese Zustände wurden dann absichtlich einem zufälligen Phasenrauschen ausgesetzt, um den Effekt einer rauschbehafteten optischen Übertragung nachzubilden. Unter Verwendung dieser Zustände wurde ein vollständiges Destillationsprotokoll experimentell umgesetzt. Die destillierten Zustände stehen für nachfolgende Experimente zur Verfügung, was im Kontrast zu früheren Experimenten im Regime diskreter Variablen („Einzelphotonen“) steht, in denen die Zustände typischerweise unter Anwendung des Protokolls zerstört wurden, was eine praktische Anwendbarkeit verhindert. Im Verlauf der Arbeiten offenbarte das Protokoll weitaus größere Komplexität und Möglichkeiten, als zunächst angenommen. Drei dieser Erweiterungen, nämlich *conjugate distillation*, *quantum channel probing* und *phase random distillation* wurden untersucht.

Stichworte: Quanteninformation, nichtklassisches Licht, Destillation

Symbole und Abkürzungen

Abkürzungen

A/D	Analog/Digital
AA	Anti-Aliasing
AR	Antireflektierend
BLIIRA	*Blue Induced Infrared Absorption*
BS	Strahlteiler
BSC	*Binary Symmetric Channel*
CP	*Conjugate Purification*
CV	*Continuous Variables*
DSP	*Digital Signal Processing*
EOM	Elektrooptischer Modulator
FFT	*Fast Fourier Transform*
FIR	*Finite Impulse Response*
GRIIRA	*Green Induced Infrared Absorption*
HD	Homodyndetektor
HR	Hochreflektierend
IIR	*Infinite Impulse Response*
LCG	*Linear Congruentual Generator*
LGOCC	*Local Gaussian Operations and Classical Communication*
LO	Lokaloszillator
LOCC	*Local Operations and Classical Communication*
MUS	*Minimum Uncertainty State*
OPA	*Optical Parametric Amplification*
OPO	*Optical Parametric Oscillation*
QCP	*Quantum Channel Probing*
QKD	*Quantum Key Distribution*
RBW	*Resolution Bandwidth*

SHG	*Second Harmonic Generation*
VBW	*Video Bandwidth*

Zustände

$\|0\rangle$	Vakuumzustand
$\|n\rangle$	Fockzustand mit n Photonen
$\|\alpha\rangle$	Kohärenter Zustand
$\|\alpha, \xi\rangle$	Gequetschter kohärenter Zustand

Symbole

$\langle\hat{O}\rangle$	Erwartungswert von $\hat{O}$
$[\hat{A}, \hat{B}]$	Kommutator von $\hat{A}$ und $\hat{B}$
$\mathbb{1}$	Einheitsmatrix
α	Kohärente Anregung
$\hat{a}, \hat{a}^\dagger$	Bosonische Erzeuger- und Vernichteroperatoren
a_i	*Feedforward*-Koeffizienten
B	Eckfrequenz eines Filters
$B(x,t)$	Magnetisches Feld
b_i	*Feedback*-Koeffizienten
$\chi^{(2)}$	Nichtlinearität zweiter Ordnung
$\chi^{(3)}$	Nichtlinearität dritter Ordnung
$\Delta\hat{O}$, $V_{\hat{O}}$	Varianz von $\hat{O}$
$\hat{D}(\alpha)$	*Displacement*-Operator
ϵ_0	Elektrische Feldkonstante
$\mathcal{E}$	Außerordentliche Achse
$E(x,t)$	Elektrisches Feld
E_n	Energieeigenwert
Φ	Rauschverteilung
$\mathcal{F}$	Finesse
f_s	Sampling-Frequenz

$\hbar$	Planck-Konstante
$H(X)$	Shannon-Entropie
$H_{\text{bin}(X)}$	Binäre Entropie
$H(q(x)\|\|p(x))$	Relative Entropie
$H(X,Y)$	Verbund-Entropie
$H(X\|Y)$	Bedingte Entropie
$H(X:Y)$	Wechselseitige Entropie
$H(z)$	Transferfunktion eines Filters
$\hat{H}$, H	Hamiltonoperator, Hamiltonfunktion
i	Einfallswinkel
k	Wellenzahl
μ_0	Magnetische Feldkonstante
$\hat{n}$	Anzahloperator
ω	Kreisfrequenz, optische Frequenz
$\mathcal{O}$	Ordentliche Achse
$\hat{p}$	Alternativ: Operator der Phasenquadratur
P, $\mathcal{P}$	Erfolgswahrscheinlichkeit
$p(x)$, $q(x)$	Wahrscheinlichkeitsverteilungen
P_{marg}	Marginalwahrscheinlichkeitsverteilung
$P(V_x, V_p)$	Reinheit
Q	Schwellenwert
$\hat{\rho}$, $\hat{\sigma}$	Dichteoperatoren
r	Squeezing-Parameter, Reflektivität
σ	Standardabweichung
$\mathbf{S}$	Strahlteilermatrix
$S(\hat{\rho})$	Von Neumann-Entropie
$S(\xi)$	Squeezing-Operator
τ_g	Gruppenverzögerung
τ_ϕ	Phasenverzögerung
θ	Quadraturwinkel
t	Transmittivität
t_s	Sampling-Zeit
$\hat{U}$	Zeitentwicklungsoperator
$U(V_x, V_p)$	Unschärfeprodukt
$\mathcal{V}$	*Visibility*
$W(x,p)$	Wigner-Funktion
X, Y	Zufallsvariablen
$x(n)$, $y(n)$	Diskrete Signale
$X(t)$, $Y(t)$	Kontinuierliche Signale

$\hat{X}^{\theta}$	Quadraturoperator
$\hat{X}^{+} = \hat{X}^{\theta=0}$	Operator der Amplitudenquadratur
$\hat{X}^{-} = \hat{X}^{\theta=\pi/2}$	Operator der Phasenquadratur
$\hat{x}$	Alternativ: Operator der Amplitudenquadratur
$\hat{Y}^{+}$, $\hat{Y}^{-}$	Gedrehte Quadraturoperatoren
z^{-1}	Verzögerungsoperator

KAPITEL 1

Einführung und Überblick

1.1 Einleitung

Die Durchführung von Quanteninformations- und Quantenkommunikationsprotokollen im Regime kontinuierlicher Variablen stellt vor dem Hintergrund einer technologischen Realisierung eine ansprechende Alternative zu dem traditionellen Ansatz dar, der auf diskreten Variablen („qbits“) basiert. Die meisten Grundbausteine einer Quantenkommunikation lassen sich im Regime kontinuierlicher Variablen mit nur wenigen und vergleichsweise einfach zu handhabenden Grundkomponenten realisieren. Dazu gehören optisch parametrische Verstärker/Oszillatoren zur Erzeugung nichtklassischer Zustände, Homodyndetektion und lineare optische Komponenten wie Strahlteiler und Phasenschieber.

Neben diesen Aspekten der vergleichsweise einfachen experimentellen Umsetzbarkeit zählen die hohen erreichbaren Bandbreiten und Detektionseffizienzen (nahe bei Eins) bei der Verwendung kontinuierlicher Variablen zu den Vorteilen. Eine besondere Rolle bei der Verwendung kontinuierlicher Variablen spielen die sogenannten *gaußschen Zustände* und *gaußschen Operationen*. Als gaußsche Zustände bezeichnet man dabei solche Zustände, deren Wignerfunktionen eine gaußsche Form aufweisen, die also über eine normalverteilte Messstatistik verfügen. Gaußsche Operationen sind dann solche Operationen, unter denen die gaußsche Form der Wignerfunktion erhalten bleibt. Solchen gaußschen Operationen entsprechen zum Beispiel passive optische Komponenten, Homodyndetektion und Quetschlichtquellen.

Das Grundszenario eines jeden Quanteninformationsprokolls sieht vor, dass ein quantengestützter Kommunikationskanal zwischen räumlich weit entfernten Parteien errichtet werden soll. Ein solcher Kanal könnte etwa mit optischen Fasern realisiert werden, über die den beiden Kommunikationspartnern nichtklassische Zustände des Lichtes zur Verfügung gestellt werden. Die bei einer solchen Übertragung unausweichlich auftretende Dekohärenz beeinträchtigt jedoch die nichtklassischen Eigenschaften der übertragenen Zustände (Verschränkung oder nichtklassische Rauschunterdrückung) so stark, dass eine Umsetzung von Quantenprotokollen über realistische Distanzen ($\approx 10^3$ km) nicht mehr möglich ist.

Will man eine zuverlässige Quantenkommunikation über größere Distanz realisieren, so benötigt man einen geeigneten *quantum repeater*, der in regelmäßigen Abständen entlang des Kommunikationskanals für eine „Nachverstärkung" der nichtklassischen Eigenschaften sorgt. Eine direkte Übertragung des Funktionsprinzips eines klassischen *repeaters* ist wegen des *no-cloning theorems* nicht umsetzbar. Ein *quantum repeater* basiert dagegen auf einem Destillationsprotokoll, bei dem man versucht, aus einer großen Anzahl schwach nichtklassischer Zustände eine kleinere Anzahl stark nichtklassischer Zustände zu *destillieren*. Unglücklicherweise konnte jedoch gezeigt werden, dass im Fall verschränkter Zustände eine Destillation von gaußschen Zuständen mit gaußschen Operationen nicht bewerkstelligt werden kann („*no-go theorem*"). Ein ähnliches Theorem ist auch bezüglich der Destillation von gequetschtem Licht bewiesen worden. Demnach ist es nicht möglich, aus einer beliebigen Anzahl N gequetschter Zustände gegebener nichtklassischer Rauschunterdrückung einen Zustand mit größerer nichtklassischer Rauschunterdrückung zu destillieren.

Die Umsetzung einer Destillation gequetschter oder verschränkter Zustände macht es also prinzipiell notwendig, das gaußsche Regime an mindestens einer Stelle zu verlassen. Ein vorgeschlagenes Protokoll zur Destillation von verschränkten Zuständen sieht zum Beispiel vor, die Zustände zunächst zu degaußifizieren, etwa durch konditionierte Subtraktion eines einzelnen Photons. Bei einem solchen Vorgehen gibt man allerdings die Vorzüge kontinuierlicher Variablen auf, da das Protokoll im Wesentlichen auf einer Einzelphotonendetektion beruht.

Es ist jedoch bekannt, dass zufälliges Phasenrauschen in optischen Fasern eine prominente Rauschquelle bei der Übertragung von nichtklassischen Zuständen ist, das zum Beispiel durch Streuung des Lichtes an thermischen Phononen zustande kommt. Unter dem Einfluss eines solches Rauschens werden die beeinträchtigten Zustände zunehmend nichtgaußsch, so dass das

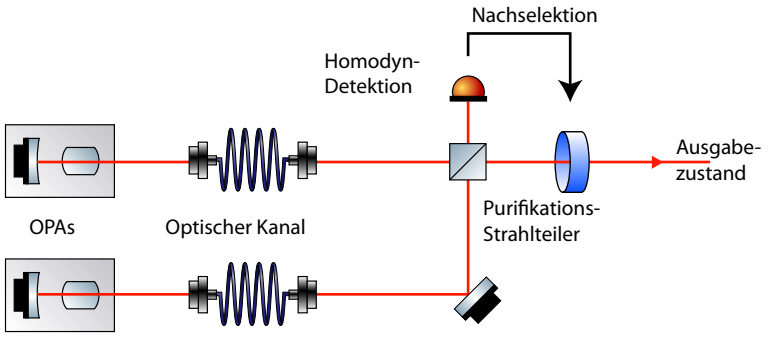

Abbildung 1.1 — Prinzipskizze eines Destillations- und Purifikationsexperimentes. Zwei Kopien eines gequetschten Zustandes werden mittels optisch parametrischer Verstärkung (OPA) präpariert. Es erfolgt eine Übertragung beider Zustände durch einen optischen Kanal, wobei die nichtklassischen Eigenschaften der beiden Zustände beeinträchtigt werden. Nach der Übertragung werden die Zustände phasenstarr auf einem Strahlteiler („Purifikationsstrahlteiler“) überlagert. Ein Ausgang des Strahlteilers wird mit einem Homodyndetektor vermessen und der zweite Ausgang wird abhängig vom Ergebnis dieser Messung manipuliert. Der so entstehende Zustand steht nun für ein nachfolgendes Experiment zur Verfügung.

„*no-go theorem*“ nicht mehr beachtet werden muss. Demnach kann nun eine Destillation gelingen, auch wenn lediglich passive optische Komponenten, Homodyndetektion und Nachselektion verwendet werden.

Das prinzipielle Vorgehen ist in ⇝Abbildung 1.1 dargestellt. Um eine Destillation von gequetschten Zuständen durchzuführen, überlagert man zwei Kopien eines phasenverrauschten (und folglich nichtgaußschen) gequetschten Zustandes phasenstarr auf einem Strahlteiler. Die beiden Zustände werden zunächst mittels optisch parametrischer Verstärkung hergestellt und dann mit zufälligem Phasenrauschen versehen (Simulation der Eigenschaften eines optischen Kanals beträchtlicher Länge). Einer der Ausgänge dieses Strahlteilers wird mit einem Homodyndetektor vermessen und der zweite Ausgang wird auf das Ergebnis dieser Messung konditioniert. Der konditionierte Zustand im zweiten Ausgang des Strahlteilers kann dann eine größere nichtklassische Rauschunterdrückung aufweisen, als jede der beiden Kopien des Zustandes vor der Überlagerung auf dem Strahlteiler.

Ein solches Protokoll zur Destillation gequetschter Zustände ist in der vorliegenden Arbeit experimentell umgesetzt und detailliert analysiert worden, wozu auch umfassende numerische Simulationen durchgeführt worden sind. Die theoretische Beschreibung, auf der das Protokoll basiert, stammt von J. Fiurášek, mit dessen Arbeitsgruppe eine erfolgreiche Zusammenarbeit gepflegt wurde.

Im Verlauf der Arbeit wurden mehrere Verbesserungen und Erweiterungen des Protokolls erdacht und ausgearbeitet. Außerdem konnte gezeigt werden, dass das vorgestellte Protokoll als Grundbaustein einer iterativen Strategie für Destillation aufgefasst werden kann, die bei Verwendung einer Anzahl $N > 2$ von Kopien des gequetschten Zustandes durch wiederholte Anwendung des Protokolls zustande kommt.

1.2 Gliederung

In Kapitel 2 werden zunächst die Grundlagen der Quanteninformationstheorie betrachtet. Dabei gehen wir von klassischer Kommunikationstheorie aus und werden die Shannon-Entropie als Maß für Information (und äquivalent für Unsicherheit) herleiten. Weitere Entropiebegriffe werden als nützliche Werkzeuge vorgestellt. Wir betrachten dann die Übertragung von Informationen über einen störungsbehafteten Kanal. Die Übertragung dieser Konzepte auf Quantenzustände wird auf die von Neumann-Entropie führen. Abschließend wird ein Überblick über das faszinierende Gebiet der Quantenkryptographie gebracht und es folgt die Vorstellung einiger grundlegender Protokolle, die in einem realistischen Szenario durch Störeigenschaften des Übertragungskanals begrenzt sind.

Nach dieser kurzen Einführung stellen wir in Kapitel 3 wichtige Eigenschaften nichtklassischer Zustände des Lichtes zusammen. Nach Einführung von Quadraturoperatoren betrachten wir vor allem die für diese Arbeit wichtigen *gequetschten Zustände* und ihre Erzeugung. Die Wignerfunktion wird – vor allem als nützliches Werkzeug zum *intuitiven Umgang* mit solchen Zuständen – vorgestellt. Nach einem historischen Überblick über die Geschichte gequetschter Zustände (die mehr als 75 Jahre in die Vergangeheit reicht) betrachten wir optische Methoden zur Erzeugung gequetschter Zustände, vor allem optisch parametrische Prozesse und die dafür benötigten nichtlinearen Kristalle mit ihren Eigenschaften.

Im Anschluss an diese beiden grundlegenden Kapitel wenden wir uns nun (Kapitel 4) der Destillation und Purifikation von Quantenzuständen zu. Es werden einige formelle Betrachtungen zu gaußschen Zuständen und gaußschen Operationen durchgeführt. Für solche Zustände und Operationen kann kein Destillationsprotokoll realisiert werden („*no-go theorem*“). Wir betrachten dann die Wirkung von Phasenrauschen auf gaußsche Zustände und können damit ein einfaches Destillationsprotokoll, das auf einer simplen Konditionierungsbedingung basiert, realisieren. Abschließend unternehmen wir den Versuch einer anschaulichen Deutung der Funktionsweise dieses Protokolls und zeigen die Ergebnisse erster Simulationen.

In Kapitel 5 befassen wir uns mit der experimentellen Umsetzung des vorgestellten Destillations- und Purifikationsprokolls für gequetschte Zustände. Die drei Grundbausteine *Erzeugung*, *Übertragung* und *Detektion*, zusammen mit einem vierten Baustein *Nachbearbeitung* (den wir bewusst von den drei Erstgenannten trennen), werden im Detail betrachtet.

Neben der experimentellen („optischen“) Realisierung spielen bei der Umsetzung des vorgestellten Destillations- und Purifikationsprotokolls eine Reihe von Techniken eine Rolle. In Kapitel 6 werden diese Techniken vorgestellt und zur Anwendung gebracht. Dazu gehört die Entwicklung der benötigten Software und Grundtechniken der digitalen Signalverarbeitung, vor allem digitale Filterungen. Neben der experimentellen Umsetzung wurden umfangreiche Simulationen und numerische Analysen zur Purifikation und Destillation gequetschter Zustände durchgeführt. Die dafür erstellte Software wird vorgestellt.

Im Kapitel 7 stellen wir experimentelle und durch numerische Simulation gewonnene Ergebnisse vergleichend gegenüber. Dabei vollziehen wir auch nach, wie verschiedene Erweiterungen des ursprünglich vorgeschlagenen Protokolls entdeckt und entwickelt wurden. Nach der detaillierten Analyse zweier dieser Erweiterungen (*conjugate purification* und *quantum channel probing*) werden die Grundlagen iterativer Strategien betrachtet.

Das abschließende Kapitel 8 liefert eine Diskussion der geleisteten Arbeit und einen Ausblick, vor allem im Hinblick auf eine Destillation von *verschränkten* Zuständen. Dabei wird auch der Vergleich gezogen mit früheren Experimenten im Regime diskreter Variablen („Einzelphotonen“).

1.3 Hinweise zur Notation

Bei der Beschäftigung mit Quantenoptik und Quanteninformationstheorie fällt auf, dass die verwendeten Notationen in der Literatur nicht einheitlich gehandhabt werden. Als Beispiel mögen die Quadraturoperatoren dienen, die manchmal als $\hat{X}^+$ und $\hat{X}^-$ definiert werden, manchmal mit einem zusätzlichen Faktor $1/\sqrt{2}$, dann als $\hat{x}$ und $\hat{p}$ bezeichnet. Andere Autoren verzichten auf den Faktor $1/\sqrt{2}$, bezeichnen aber dennoch als $\hat{x}$ und $\hat{p}$. Wieder andere definieren Quadraturoperatoren $\hat{p}$ und $\hat{q}$, manchmal *mit* und manchmal *ohne* zusätzliche Faktoren $1/\sqrt{2}$ oder gar $1/2$, wodurch es sogar zu einer Überschneidung des Symbols $\hat{p}$ zwischen den Notationen kommt.

In der vorliegenden Arbeit wird eine lokal optimierte Nomenklatur verwendet, d. h. innerhalb eines Kapitels ist die Notation vereinheitlicht. In jedem Fall verwenden wir eine Normierung der Art, dass das Vakuumrauschen bei einem Wert von Eins liegt.

1.4 Hinweise zu Anglizismen

Es wird generell versucht, die Verwendung von Anglizismen zu vermeiden. An verschiedenen Stellen wird jedoch aus einem von zwei möglichen Gründen von dieser Bemühung abgesehen. Wenn zu einem Begriff keine verbreitete deutsche Entsprechung existiert, wird *nicht* der Versuch unternommen, eine zu schaffen. Dies betrifft vor allem die Bezeichnung von Verfahren, die bisher ausschließlich in englischer Sprache publiziert worden sind. Einige Begriffe wurden zum Beispiel im Rahmen der vorliegenden Arbeit überhaupt erst geprägt (etwa *quantum channel probing*). Ein Übersetzungsversuch scheint nicht sinnvoll und unterbleibt.

Weiterhin weichen wir auf einen Anglizismus aus, wenn die englische Bezeichnung gegenüber ihrer deutschen Entsprechung eine *andere* oder *weitergehende* Bedeutung aufweist. In beiden Fällen bringen wir den bedachten Umgang mit solchen Worten durch eine besondere Auszeichnung zum Ausdruck: Anglizismen kommen in englischer Rechtschreibung und *kursiv* daher.

Eine einzige Ausnahme wird beim gequetschten (*squeezed*) Licht gemacht, das mit Quetschlichtquellen (*squeezers*) erzeugt wird. Die Begriffe *squeezing* (synonym verwendet für den Vorgang des Quetschens von Licht, die resultierenden gequetschten Zustände und die Stärke der nichtklassischen Rausch-

unterdrückung[1]) und *squeezer* als Bezeichnung für die Quetschlichtquelle sind inzwischen derart gebräuchlich, dass sie ihre deutschen Gegenstücke im Sprachgebrauch fast völlig verdrängt haben. Wir betrachten diese Bezeichnungen nicht länger als Anglizismen. Ab hier also: „Squeezing“ und „Squeezer“ statt *„squeezing“* und *„squeezer“*.

1.5 Hinweise zur Passivform

Manche Autoren sind der Ansicht, dass eine wissenschaftliche Arbeit grundsätzlich in der Passivform („Es wird davon ausgegangen, dass…“) formuliert werden muss. Diese Grundregel führt in der Praxis manchmal zu extrem sperrigen Formulierungen, wodurch die aktive Formulierung („Wir gehen davon aus, dass…“) gerechtfertigt wird. Falls nun die vorliegende Arbeit lediglich von einem einzigen Autor verfasst worden ist, wirkt diese Art zu Formulieren allerdings ein wenig anmaßend. Die in diesem Fall richtige Singularform („Ich gehe davon aus, dass…“) hat (wenigstens im Deutschen) einen recht informellen Charakter, der häufig nicht angemessen erscheint. Als Ausweg bietet sich der folgende Kompromiss an: Es wird prinzipiell die Passivform bemüht. Um lesefreundlichere Formulierungen zu ermöglichen, wird die „Wir“-Form gelegentlich verwendet, allerdings nur genau dann, wenn dadurch „der Leser und der Autor“ referenziert wird. Nachdem also eine „Gleichung aufgeschrieben wurde“, können „wir nun nachvollziehen, dass…“.

[1] Wenn man also sehr gute Squeezer baut, gelingt das Squeezing so gut, dass man Squeezing mit sehr viel Squeezing herstellen kann.

KAPITEL 2

Grundlagen der Quantenkommunikation

2.1 Klassische Informationstheorie

Das Grundkonzept klassischer Informationstheorie (die eigentlich eine *Kommunikationstheorie* ist) kann man sich am Beispiel eines alltäglichen Vorgangs verdeutlichen. Wir betrachten dazu zwei Menschen, wobei einer der beiden im Besitz einer *Nachricht* ist, die er dem zweiten gerne zukommen lassen würde. Dazu benötigt es offenbar eine Kommunikation zwischen beiden Menschen, die gewöhnlich mittels *Sprache* stattfindet. Die natürliche Konstruktion einer geeigneten Sprache spiegelt dabei Konzepte klassischer Informationstheorie wieder. Es ist etwa klar, dass häufig auftauchende Worte („ich“, „ein“) generell *kürzer* sein sollten, als weniger häufig verwendete („Autobahnabfahrt“, „Quanteninformationstheorie“). Damit wird dem Anspruch der Effizienz Rechnung getragen. Weiter spielen Eigenschaften des *Kommunikationskanals* eine Rolle. Stehen die beiden Menschen etwa auf unterschiedlichen Seiten einer vielbefahrenen Straße, kann es passieren, dass Teile der Nachricht durch den Lärm eines vorbeifahrenden Fahrzeugs *nicht verstanden* oder *falsch verstanden* werden. In diesem Fall stellt man den Anspruch, dass selbst im Fall *nicht perfekter Übertragung* die ursprüngliche Nachricht – wenigsten teilweise – rekonstruiert werden kann. Die Informationstheorie, deren Grundlagen wir im Folgenden darstellen werden, betrachtet dabei nicht die *Wichtigkeit* einer Nachricht oder ihrer Teile. Im Fall des eben zitierten Beispiels einer fehlerhaften

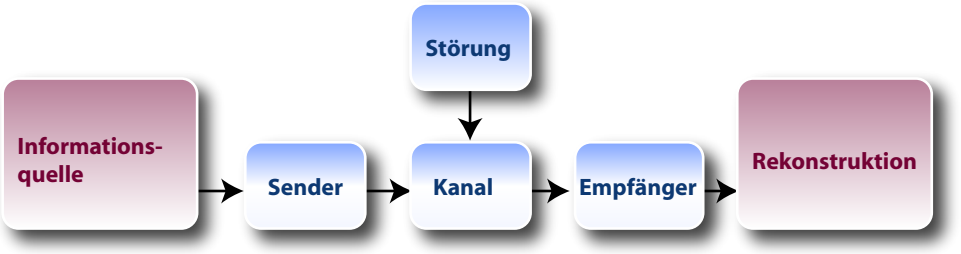

Abbildung 2.1 — Ein abstraktes Kommunikationsmodell. Eine Informationsquelle kann eine definierte Menge von Nachrichten generieren. Eine dieser Nachrichten wird vom Sender über einen Kanal, der im Allgemeinen dem Einfluss von Störungen ausgesetzt sein kann, zu einem Empfänger übertragen, der die Nachricht zu rekonstruieren versucht. Der Kanal muss in gleicher Weise für jede Nachricht funktionieren, die die Informationsquelle produzieren kann. Der *Bedeutungsinhalt* der Nachricht wird im Rahmen der Informationstheorie nicht betrachtet.

Übertragung einer Nachricht, macht es einen gewaltigen Unterschied, welcher Teil der Nachricht beeinträchtigt wird: Während die empfangene Nachricht „Ruf schnell einen [...]!“ für den *Emfänger* praktisch wertlos ist, kann aus „[...] schnell einen Krankenwagen!“ durchaus das Anliegen des *Senders* rekonstruiert werden. Dieser Umstand wird im Rahmen der Informationstheorie *nicht* betrachtet!

Das Konzept von *Kommunikation* soll nun abstrahiert werden. Die Disziplin der klassischen Informationstheorie wurde von Claude Shannon 1948 [Sha48] begründet. Ein abstraktes Modell einer Kommunikation (⇝Abbildung 2.1) sieht vor, dass an einem Ort eine Nachricht (exakt oder näherungsweise) rekonstruiert werden soll (*Empfänger*), die an einem anderen Ort (*Sender*) ausgewählt worden ist. Die Nachricht selber trägt dabei *Bedeutung*. Diese wird in der Informationtheorie zwar nicht betrachtet, symbolisiert aber konzeptionell, dass die Nachricht irgendeiner *Informationsquelle* entstammt (etwa einem physikalischen System, dessen Eigenschaften gemessen wurden, wobei das Messergebnis nun in Form einer Nachricht mitgeteilt werden soll). Entscheidend ist dabei, dass der Kommunikationskanal in *gleicher Weise* für jede ausgewählte Nachricht, die die Informationsquelle produzieren kann, funktionieren muss.

2.1.1 Information und Unsicherheit

Zwischen den beiden Begriffen der *Information* und der *Unsicherheit* gibt es einen engen Zusammenhang. Man stelle sich eine Maschine vor, die eins der drei Symbole A, B oder C produzieren kann, jedes der drei mit der gleichen Wahrscheinlichkeit $p = 1/3$. Während wir auf die Ausgabe des nächsten Symbols warten, haben wir eine gewisse Unsicherheit bezüglich der Frage, welches Symbol sich realisieren wird. Ist die Ausgabe dann erfolgt, so kennen wir das Ergebnis und haben dabei Information gewonnen. Die Unsicherheit, die man über die Identität des nächsten Symbols hat, wird durch die Information über seine Identität beseitigt. Wir wollen die Unsicherheit und den Informationsgewinn quantifizieren. Eine Möglichkeit besteht darin anzugeben, die Unsicherheit betrage im obigen Beispiel vor der Realisierung des nächsten Symbols „drei Symbole“. Dieser Ansatz hat aber einen Nachteil: Man verfügt zum Beispiel über eine zweite Maschine, die die Symbole 1 und 2 gleichverteilt realisieren kann (Unsicherheit „zwei Symbole“). Kombiniert man nun die Symbolausgabe der beiden Maschinen zu $A1$, $A2$, $B1$, $B2$, $C1$ und $C2$, so entspräche dies einer Unsicherheit von „sechs Symbolen“ bezüglich der Ausgabe des nächsten Symbolpaares. Die Unsicherheit ist in dieser Definition also kein *additives Maß*. Dies jedoch widerspricht unserer intuitiven Vorstellung von Information: Wird ein Text in seiner Länge verdoppelt, stellen wir uns vor, dass er die „doppelte“ Information beinhalten kann. Wir definieren die Unsicherheit, wenn wir uns einer Maschine gegenübersehen, die gleichverteilt eins von M Symbolen realisieren kann besser als

$$U = \log(M). \tag{2.1}$$

Die Logarithmusbildung hat dabei den Vorteil der Additivität. Im obigen Beispiel der beiden Maschinen beträgt die Gesamtunsicherheit $U = \log(3) + \log(2) = \log(6)$. Die *Maßeinheit* der Unsicherheit wird dabei durch die Basis des Logarithmus vorgegeben. Arbeitet man mit einem Logarithmus zur Basis 2, so spricht man von *„binary digits“* oder abgekürzt *bits*. Im Fall der Maschine, die die beiden Symbole 1 und 2 realisieren kann, beträgt die Unsicherheit dann $U = \log_2(2) = 1$ bit. Hat man eine Maschine, die lediglich ein einziges Symbol produzieren kann, beträgt die Unsicherheit bezüglich des nächsten Symbols $U = \log_2(1) = 0$. Es besteht keine Unsicherheit über die Identität des nächsten Symbols.

Da die Realisierung eines Symbols genau die Ungewissheit U beseitigt,

definieren wir als Information

$$I = U = \log_2(M) = -\log_2\left(\frac{1}{M}\right) = -\log_2(P), \tag{2.2}$$

wobei $P = 1/M$ die Wahrscheinlichkeit für die Realisierung eines Symbols bezeichnet. Eine Sequenz von N gleichverteilten Symbolen enthält folglich wegen der Additivität genau die Information

$$I = N\log_2(M) = \log_2\left(M^N\right). \tag{2.3}$$

Wir verallgemeinern dieses Ergebnis nun für den Fall *nicht gleichverteilter* Wahrscheinlichkeiten für die Realisierung eines Symbols. Aus einer Reihe von M möglichen Symbolen bezeichne $u_j = i_j$ analog die Information, die bei Realisierung des Symbols j erhalten wird:

$$i_j = -\log_2(P_j). \tag{2.4}$$

In einer langen Sequenz von N Symbolen realisiert sich ein Symbol, das mit einer Wahrscheinlichkeit P_j auftritt durchschnittlich N_j mal, wobei $N_j/N = P_j$ ist. Der durchschnittliche Informationsgewinn pro Symbol beträgt dann

$$H = \sum_{j=1}^{M} \frac{N_j}{N} i_j = \sum_{j=1}^{M} P_j i_j. \tag{2.5}$$

Setzt man noch ⇝Gleichung (2.4) für i_j ein, erhält man die sogenannte *Shannon-Entropie*

$$H = -\sum_{j=1}^{M} P_j \log_2(P_j). \tag{2.6}$$

Betrachtet man die Form von H für den Fall $M = 2$ (⇝Abbildung 2.2), so erkennt man, dass der Informationsgewinn pro Symbol genau dann maximal ist, wenn Gleichverteilung der Wahrscheinlichkeiten vorliegt: $P_1 = P_2 = 1/2$. Dieses Ergebnis gilt qualitativ auch für den Fall *vieler* Symbole. Stets ist der Informationsgewinn (ebenso wie die Unsicherheit bezüglich des nächsten Symbols) maximal im Fall gleichverteilter Wahrscheinlichkeiten. *Maximale Unsicherheit bietet das größte Potential für Informationsgewinn*[1].

[1] Ist etwa bekannt, dass ein Symbol nur mit verschwindend geringer Wahrscheinlichkeit auftritt, entspricht dies einer *a priori* Information: Wir sind sehr sicher, dass sich dieses Symbol nicht realisieren wird.

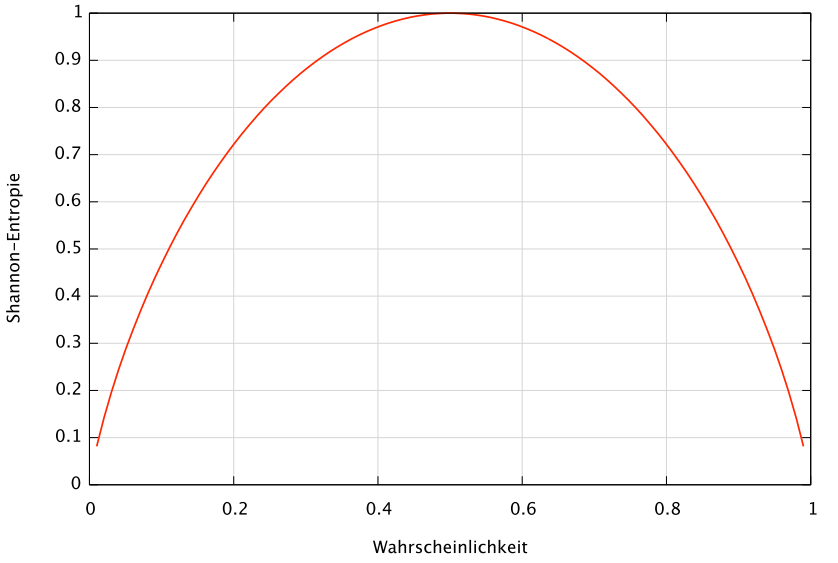

Abbildung 2.2 — Shannon-Entropie $H(P_1)$ für den Fall zweier Symbole. Für die Wahrscheinlichkeit des zweiten Symbols gilt $P_2 = 1 - P_1$. Die Shannon-Entropie wird maximal, falls $P_1 = P_2 = 1/2$.

Die Bedeutung der Shannon-Entropie kann am folgenden Beispiel erfaßt werden. Shannon stellte sich die Frage, welche Menge an *Resourcen* notwendig ist, um eine Nachricht derart zu speichern, dass sie zu einem späteren Zeitpunkt vollständig rekonstruiert werden kann. Um diese Frage zu untersuchen, betrachten wir eine Maschine, die die vier Symbole A, B, C und D realisieren kann. Die zugehörigen Wahrscheinlichkeiten seien *nicht* gleichverteilt und lauten

$$P_A = 1/2, \quad P_B = 1/4, \quad P_C = P_D = 1/8. \tag{2.7}$$

Zum Kodieren einer Nachricht, die aus diesen vier Symbolen zusammengesetzt werden kann, werden zwei Bits Speicherplatz pro Symbol benötigt. Es wird beim Betrachten aber sofort klar, dass man eine aus diesen Symbolen zusammengesetzte Nachricht möglicherweise resourcengünstiger kodieren kann, wenn man bedenkt, dass das Symbol A viel häufiger auftauchen wird als das Symbol D. Wir betrachten zum Beispiel eine Nachricht aus acht Symbolen, die mit dieser Maschine erzeugt worden ist:

$$A\,B\,A\,D\,C\,A\,A\,B. \tag{2.8}$$

Da das A (gemäß seiner Wahrscheinlichkeit) häufig vorkommt, sollten wir versuchen, dieses Symbol mit weniger Bits zu kodieren, als das selten vorkommende D. Eine Möglichkeit der Kodierung besteht etwa in der Verwendung der folgenden binären Ausdrücke:

$$\begin{array}{lll} A = & 0 & (1\text{ bit})\,, \\ B = & 00 & (2\text{ bit})\,, \\ C = & 110 & (3\text{ bit})\,, \\ D = & 111 & (3\text{ bit})\,. \end{array} \tag{2.9}$$

Damit kann dieselbe Nachricht (⇝Gleichung (2.8)) auch durch die binäre Sequenz

$$01001111100010 \tag{2.10}$$

dargestellt werden. Wir können den durchschnittlich benötigten Speicherplatz pro Symbol berechnen, indem wir den für jedes Symbol benötigten Speicherplatz mit den entsprechenden Wahrscheinlichkeiten gewichten: $(1/2) \times 1 + (1/4) \times 2 + (1/8) \times 3 + (1/8) \times 3 = 7/4$ Dies ist offenbar weniger, als die 2 bits pro Symbol, die wir in der ursprünglichen Darstellung (⇝Gleichung (2.8)) benötigten. Wir können nun die Shannon-Entropie der *ursprünglichen Darstellung* berechnen und finden:

$$H(X) = ... = 7/4. \tag{2.11}$$

Man kann zeigen, dass jeder Versuch, die Nachricht weiter zu komprimieren, unweigerlich einen Informationsverlust mit sich bringt. Die Shannon-Entropie gibt also den benötigten Speicherplatz bei bestmöglich erreichbarer Komprimierung einer Nachricht an. Dieser Sachverhalt ist als *Shannon's noiseless coding theorem* bekannt geworden.

Die Shannon-Entropie nimmt, wie wir gesehen haben, ab, falls keine Gleichverteilung der Symbole gegeben ist. Ausserdem nimmt die Shannon-Entropie ab, falls es statistische Korrelationen zwischen aufeinanderfolgenden Symbolen gibt. Beides ist in jeder realen Sprache der Fall. Im Deutschen etwa kommt der Buchstabe *e* wesentlich häufiger vor, als der Buchstabe *x*. Ebenso folgt auf ein *e* mit größerer Wahrscheinlichkeit ein *t* als ein *z*.

Aus dieser Beobachtung folgt, dass eine reale Sprache keine optimale Kodierung der zu übermittelnden Nachricht liefert. (Wobei wir außer Acht lassen, dass in jeder in realer Sprache formulierten Nachricht weitere Information „zwischen den Zeilen“ verborgen ist).

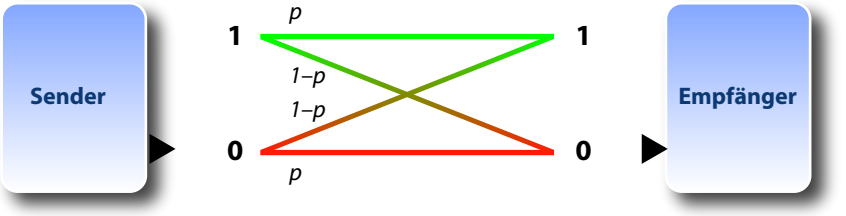

Abbildung 2.3 — Gestörte Übertragung: Sendet der Sender eine „1“, so wird mit der Wahrscheinlichkeit p auch eine „1“ empfangen, mit der Wahrscheinlichkeit $1-p$ jedoch fälschlicherweise eine „0“. Gelten dieselben Wahrscheinlichkeiten umgekehrt auch für das andere mögliche Symbol, so spricht man von einem *binären, symmetrischen Kanal* (BSC).

2.1.2 Rauschbehafteter Kanal

Wir betrachten nun das Problem der *Übertragung* einer Nachricht. Dazu stellen wir uns vor, dass auf Seiten eines Senders eine Nachricht aus N Symbolen aus dem Alphabet $\{1,0\}$ präpariert wurde, die nun durch einen Kanal übertragen werden soll. Geschieht diese Übertragung mit einer Rate von einem Symbol pro Sekunde, beträgt die Kapazität offenbar 1 bit/s. Wir stellen uns nun vor, dass der Übertragungskanal die Nachricht verfälscht. Wenn eine 0 gesendet wird, so betrage die Wahrscheinlich dafür, dass auch eine 0 empfangen wird 0,99. Mit einer Wahrscheinlichkeit von 0,01 wird fälschlicherweise eine 1 empfangen. In gleicher Weise beträgt die Wahrscheinlichkeit für den Empfang einer 1 wenn eine 1 gesendet wurde 0,99 (binärer, symmetrischer Kanal – siehe auch ⇝Abbildung 2.3). Demnach beträgt die Unsicherheit, nachdem ein einzelnes Symbol empfangen worden ist $H = -0{,}99\log_2(0{,}99) - 0{,}01\log_2(0{,}01) = 0{,}081$. Die effektive Kapazität des Kanals hat also auf $1 - 0{,}081 = 0{,}919$ bit/s abgenommen. Hierbei betrachten wir zunächst nicht, welche Möglichkeiten es gibt, die falsch übertragenen Bits zu identifizieren oder vielleicht sogar zu korrigieren (*error correction*).

2.1.3 Entropie

Nach der Einführung der letzten beiden Abschnitte wollen wir nun etwas technischer vorgehen und die Bedeutung und Eigenschaften der Entropie genauer untersuchen. Wir betrachten im folgenden Zufallsvariablen X und Y. Diese können je einen der d Werte $x_1, \ldots, x_d$ annehmen. Die Gesamtheit der Werte $\{x_1, \ldots, x_d\}$ bezeichnen wir als ein *Alphabet* der *Länge* d. Einer der Werte des Alphabets wird als *Buchstabe* bezeichnet, eine „Nachricht", die aus einer Aneinanderreihung (Sequenz) von Buchstaben besteht, nennt man ein *Wort*.

Wir hatten Bereits die Shannon-Entropie definiert als Maß für die Unsicherheit bezüglich der Realisierung des nächsten Buchstabens eines Wortes *bevor* diese stattfindet, bzw. äquivalent als Maß für den Informationsgewinn *nach* der Realisierung. Der Vollständigkeit halber geben wir die Shannon-Entropie erneut an:

$$H(X) = -\sum_x p_x \log(p_x). \tag{2.12}$$

Die Summe läuft dabei über alle Buchstaben des Alphabetes X und p_x bezeichnet die Wahrscheinlichkeit für die Realisierung des Buchstabens x. Wir schreiben ab jetzt die Basis des Logarithmus nicht mehr mit an, falls es sich um die Basis 2 handelt. Als Spezialfall der Shannon-Entropie hatten wir ebenfalls bereits die *binäre Entropie* aufgeschrieben, die man erhält, wenn das betrachtete Alphabet lediglich über zwei Buchstaben verfügt („Münzwurf"):

$$H_{\text{bin}}(X) = -p\log(p) - (1-p)\log(1-p) \quad [H(p) = H(1-p)]. \tag{2.13}$$

Wir hatten gesehen, dass die binäre Entropie $H_{\text{bin}}(X)$ maximal wird für $p = 1/2 = (1-p)$ (siehe auch ⇝Abbildung 2.2).

Wir betrachten nun den Fall zweier Wahrscheinlichkeitsverteilungen $p(x)$ und $q(x)$ über demselben Alphabet. Für diese beiden Verteilungen definieren wir die *relative Entropie*, die ein Maß für die Ähnlichkeit der beiden Verteilungen darstellt:

$$\begin{aligned} H(p(x)||q(x)) &= \sum_x p(x)\log\left(\frac{p(x)}{q(x)}\right) \\ &= -H(X) - \sum_x p(x)\log(q(x)). \end{aligned} \tag{2.14}$$

Die relative Entropie ist nichtnegativ und genau dann gleich Null, wenn $q(x) = p(x)$. Aus dieser Definition kann man unmittelbar Nutzen ziehen,

wenn man den Fall betrachtet, dass $p(x)$ irgendeine Verteilung ist und $q(x) = 1/d$ gleichverteilt sein soll. Berechnet man in diesem Fall die relative Entropie, findet man

$$\begin{aligned} H(p(x)||q(x)) = H(p(x)||1/d) &= -H(X) - \sum_x p(x)\log(1/d) \\ &= \log(d) - H(X). \end{aligned} \tag{2.15}$$

Weil nun aber die relative Entropie nichtnegativ ist, ist auch

$$\log(d) - H(X) \geq 0. \tag{2.16}$$

Der Fall der Gleichheit realisiert sich, falls $p(x)$ ebenfalls eine Gleichverteilung ist. Dann gilt

$$H(X) = \log(d). \tag{2.17}$$

Dieses Ergebnis hatten wir vorher bereits für Spezialfälle erhalten. Betrachtet man etwa wieder den Fall eines Alphabetes der Länge $d = 2$, etwa $\{0, 1\}$, so berechnet man (im Fall der Gleichverteilung) die Shannon-Entropie einzig aus der Länge des Alphabetes zu $H(X) = \log(d) = \log(2) = 1$. Es wird damit klar, warum in der gewohnten binären Darstellung einer Nachricht, „ein Bit" genau ein bit Information trägt.

Wir untersuchen nun den Fall zweier Zufallsvariablen X und Y. Die *Verbundwahrscheinlichkeitsverteilung* $p(x, y)$ gibt die Wahrscheinlichkeit an, dass X den Wert x annimmt und gleichzeitig Y den Wert y hat. Mit dieser Grundlage definiert man die *Verbundentropie* analog zur Shannon-Entropie als

$$H(X, Y) = -\sum_{x,y} p(x, y)\log(p(x, y)). \tag{2.18}$$

Sie gibt die Unkenntnis über das Wertepaar (X, Y) an. Nehmen wir nun an, dass der Wert von Y aus dem Paar (X, Y) bereits bekannt ist. In diesem Fall verfügen wir bezüglich der Identität des Paares $H(X, Y)$ bereits über eine gewisse Information, die durch $H(Y)$ quantifiziert wird. Damit folgt sofort eine Definition für die *bedingte Entropie* von X bei Kenntnis von Y:

$$H(X|Y) = H(X, Y) - H(Y). \tag{2.19}$$

Die bedingte Entropie gibt die durchschnittliche Unsicherheit über den Wert von X bei gleichzeitig bereits bekanntem Wert von Y an.

Als letztes Konzept führen wir die sogenannte *wechselseitige Information* ein. Sie ist ein Maß für den gemeinsamen Informationsgehalt der Zufallsvariablen

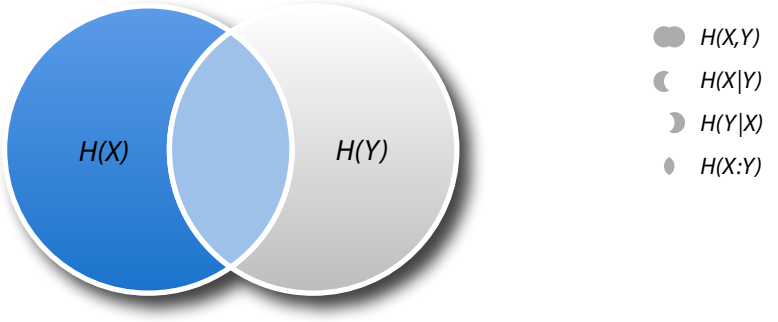

Abbildung 2.4 — Visualisierung der verschiedenen Entropie-Begriffe. Die Abbildung ist im mathematischen Sinne nicht präzise, leistet aber sehr gute Dienste als Merkhilfe.

X und Y. Die Herleitung ist einfach: Addiert man den Informationsgehalt von X, also $H(X)$, und Y, also $H(Y)$, so wird in dieser Summe die gemeinsame Information von X und Y doppelt berücksichtigt, Informationen, die nur in X oder nur in Y enhalten sind, jedoch nur einmal. Subtrahiert man von dieser Summe die Verbundentropie, so erhält man das gewünschte Maß:

$$H(X:Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y). \tag{2.20}$$

Vergleicht man die linke mit der rechten Seite dieser Gleichung und formt geeignet um, erhält man

$$H(X) = H(X:Y) + H(X|Y). \tag{2.21}$$

Hieraus kann man die wichtige *data processing inequality* ablesen. Es ist nämlich $H(X) \geq H(X:Y)$, und zwar um einen Betrag $H(X|Y)$. Man denke nun an eine Situation, in der auf Seiten eines Senders eine Nachricht X vorbereitet und an einen Empfänger übertragen wird. Dieser erhält eine Nachricht Y, die sich im Fall eines störungsbehafteten Kanals von X unterscheiden kann. Wir fragen nun, ob der Empfänger eine Möglichkeit hat, die ursprüngliche Nachricht X zu rekonstruieren, ohne einen Informationsverlust zu erleiden. Dies geht offenbar genau dann, wenn mit der Kenntnis eines Symbols aus Y *keine* Unkenntnis über das zugehörende Symbol aus X verbunden ist, wenn also genau $H(X|Y) = 0$ gilt. In diesem Fall gilt in der *data processing inequality* der Fall der Gleichheit. Wenn durch eine Datenverarbeitung auf Seiten des Empfängers die ursprüngliche Nachricht nicht rekonstruiert werden kann,

tritt zwangsläufig ein Informationsverlust ein. Genau dieser Umstand wird durch die *data processing inequality* zum Ausdruck gebracht.

Für eine graphische Veranschaulichung der verschiedenen Entropie-Begriffe betrachte man das Diagramm in ⇝Abbildung 2.4.

2.2 Quanteninformation

2.2.1 Quantenzustände und Entropie

Wir wollen in diesem Abschnitt die Ergebnisse des vorigen Abschnitts auf Quantenzustände übertragen. Dabei werden wir sehen, dass die Anwendung von Konzepten der klassischen Informationstheorie auf Quantenzustände Folgerungen nach sich zieht, die in der klassischen Theorie nicht existieren. Es sind genau diese Besonderheiten, die die Quanteninformationstheorie ausnutzt, um klassisch nicht realisierbare Protokolle umzusetzen.

Während wir im vorangegangenen Abschnitt mit klassischen Wahrscheinlichkeitsverteilungen gearbeitet haben, wollen wir nun den Dichteoperator $\hat{\rho}$ verwenden, der alle Informationen über einen Quantenzustand enthält. Ein solcher Dichteoperator ist ein hermitescher Operator mit den folgenden wichtigen Eigenschaften:

$$\hat{\rho} \geq 0, \quad \mathrm{tr}(\hat{\rho}) = 1, \quad \hat{\rho} = \hat{\rho}^{\dagger}. \tag{2.22}$$

Führt man an einem Quantenzustand, der durch $\hat{\rho}$ beschrieben wird, eine Messung der Observablen $\hat{A}$ durch, so erhält man als Erwartungswert

$$\langle \hat{A} \rangle = \mathrm{tr}(\hat{A}\hat{\rho}). \tag{2.23}$$

Betrachtet man einen Quantenzustand in einem endlich-dimensionalen Hilbertraum der Dimension d und ist $\{|0\rangle, \ldots |d\rangle\}$ eine Basis dieses Hilbertraumes, so kann der Dichteoperator dieses Zustandes geschrieben werden als

$$\hat{\rho} = \sum_{i,j=1}^{d} \rho_{i,j} |i\rangle \langle j| . \tag{2.24}$$

In perfekter Analogie zur Shannon-Entropie definiert man für einen Quantenzustand ρ die *von Neumann-Entropie* S:

$$S(\hat{\rho}) = -\mathrm{tr}(\hat{\rho} \log(\hat{\rho})). \tag{2.25}$$

Die Ähnlichkeit zur Shannon-Entropie wird noch deutlicher, wenn man mit ρ_x die Eigenwerte des Operators $\hat{\rho}$ bezeichnet. Dann schreibt sich die von Neumann-Entropie

$$S(\hat{\rho}) = -\sum_x \rho_x \log(\rho_x). \tag{2.26}$$

Ein nützliches Werkzeug ist die quantenmechanische Version der relativen Entropie. Diese definiert man wiederum ganz analog zu ihrem klassischen Gegenstück für zwei Dichteoperatoren $\hat{\rho}$ und $\hat{\sigma}$:

$$S(\hat{\rho}||\hat{\sigma}) = \mathrm{tr}(\hat{\rho}\log(\hat{\rho})) - \mathrm{tr}(\hat{\sigma}\log(\hat{\sigma})). \tag{2.27}$$

Man kann auch hier wieder zeigen, dass $S(\hat{\rho}||\hat{\sigma}) \geq 0$ mit dem Fall der Gleichheit genau falls $\hat{\rho} = \hat{\sigma}$. Ebenso wie im klassischen Fall ist die von Neumann-Entropie nichtnegativ und in einem d-dimensionalen Hilbertraum niemals größer als $\log(d)$.

Analog zu den klassischen Begriffen definiert man Verbund-Entropie, bedingte Entropie und wechselseitige Information. Dazu betrachtet man zwei Quantensysteme A und B, die durch einen gemeinsamen Dichteoperator $\hat{\rho}^{AB}$ beschrieben werden können. Dann definiert man:

$$\begin{aligned} S(A,B) &= -\mathrm{tr}(\hat{\rho}^{AB}\log(\hat{\rho}^{AB})), & (2.28)\\ S(A|B) &= S(A,B) - S(B), & (2.29)\\ S(A:B) &= S(A) + S(B) - S(A,B). & (2.30) \end{aligned}$$

Zwischen dem klassischen Begriff der Shannon-Entropie und dem quantenmechanischen Begriff der von Neumann-Entropie bestehen – trotz analoger Definition – weitreichende Unterschiede. Dies sei zunächst an einem Beispiel demonstriert. Man kann für die Shannon-Entropie leicht zeigen, dass $H(X) \leq H(X,Y)$ gilt. Dies ist auch anschaulich klar: Man kann über eine Zufallsvariable X nicht unsicherer sein als über das Paar (X,Y). Die angegebene Ungleichung muß für Quantenzustände jedoch nicht unbedingt gelten. Als Beispiel betrachten wir den reinen Zustand

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.31}$$

Für diesen Zustand findet man leicht $S(A,B) = 0$. Andererseits lautet der Dichteoperator von System A schlicht $\mathbb{1}/2$, somit hat das System A eine Entropie von $S(A) = 1$! Man kann auch umformulieren und sagen, dass das zusammengesetzte System eine negative bedingte Entropie aufweist: $S(A|B) = S(A,B) - S(A) < 0$.

2.2.2 Zugängliche Information

Wir wollen nun einige der Spezialitäten betrachten, die eine quantengestützte Kommunikation gegenüber einer klassischen Kommunikation aufweist. Dabei wird der Begriff der *zugänglichen Information* eine Rolle spielen. Wir betrachten dazu ein Szenario, in dem ein Sender eine Nachricht, die aus lediglich einem Symbol $X = 0, \ldots, n$ besteht, vorbereitet. Das Symbol wird dabei gemäß einer Wahrscheinlichkeitsverteilung $p_0, \ldots, p_n$ aus dem Alphabet gewählt. Dieses Symbol wird an einen Empfänger übertragen, dessen Aufgabe darin besteht, herauszufinden, welches Symbol X ihm zugestellt worden ist. Vorausgesetzt, dass ein störungsfreier Kanal zwischen Sender und Empfänger besteht, ist diese Aufgabe in einem klassischen Szenario stets zu bewerkstelligen. Als Maß dafür, wie gut die Rekonstruktion des gesendeten Symbols gelingt, kann man die wechselseitige Information $H(X : Y)$ verwenden. Wir hatten in einem früheren Abschnitt die *data processing inequality* betrachtet. Aus dieser Ungleichung wissen wir, dass die Rekonstruktion des Ursprungssymbols genau dann gelingt, wenn $H(X : Y) = H(X)$, wenn also eine eindeutige Zuordnung $Y \to X$ existiert. Die Aufgabe des Empfängers besteht also darin, das empfangene Symbol Y so zu vermessen, dass $H(X : Y)$ möglichst gleich zu $H(X)$ wird. Die bei *geschicktester Vorgehensweise* maximal erhaltbare wechselseitige Information $H(X : Y)$ bezeichnen wir als die dem Empfänger *zugängliche Information*.

Die Informationsübertragung soll nun in unserem Szenario per Quantenzuständen erfolgen. Das heißt, nachdem der Sender ein Symbol X gewählt hat, wird er, statt dieses Symbol nun „direkt“ zu übertragen, einen Quantenzustand per Zuordnungstabelle $X = 0, \ldots, n \to R = \hat{\rho}_0, \ldots, \hat{\rho}_n$ präparieren und statt des Symbols diesen Quantenzustand $\hat{\rho}$ übertragen. Unter der Vorraussetzung, dass dem Empfänger die Zuordnungsvorschrift „Symbol $\to$ Quantenzustand“ ebenfalls bekannt ist, reduziert sich die Aufgabe nun darauf, durch eine Messung festzustellen, welchen Quantenzustand der Empfänger erhalten hat. Ein Beispiel zur Illustration: Wir nehmen an, dass das Alphabet des Senders aus drei Symbolen besteht, die wir 0, 1 und 01 nennen. Die Kodierungsvorschrift lautet $0 \to |0\rangle$, $1 \to |1\rangle$ und $01 \to 1/\sqrt{2}(|0\rangle + |1\rangle)$. Offenbar wird der Empfänger in diesem Szenario Schwierigkeiten haben, durch eine Projektionsmessung die Indentität des Zustandes in Erfahrung zu bringen. Misst er etwa eine 1, bleibt die Frage, ob das Symbol 1 oder das Symbol 01 gemeint ist und ähnlich für den Fall einer Messung der 0. Ein Ausweg bestünde darin, dass der Empfänger von dem Zustand, den er erhalten hat, *viele* Kopien anfertigt und an jeder Kopie eine Messung vollzieht. Misst

er dabei stets eine 1, so weiß er mit großer Gewißheit, dass der Zustand $|1\rangle$ übertragen wurde. Mißt er an der Hälfte der Zustände eine 0 und an der anderen Hälfte eine 1, so ist das Symbol 01 übertragen worden, usw.

Diese Strategie ist aber durch das *no-cloning theorem* von vorn herein zum Scheitern verurteilt, wie man leicht einsieht. Dazu betrachtet man einen unbekannten Quantenzustand $|\phi\rangle$. Aufgabe ist es, von diesem eine Kopie anzufertigen. Das Kopieren soll dabei von einem unitären Operator $\hat{U}$ erledigt werden. Zusätzlich zu $|\phi\rangle$ benötigen wir einen zusätzlichen Ausgangszustand $|A\rangle$. Eine Quantenkopiermaschine würde dann in der folgenden Weise wirken:

$$|\phi\rangle \otimes |A\rangle \rightarrow \hat{U}(|\phi\rangle \otimes |A\rangle) = |\phi\rangle \otimes |\phi\rangle \,. \tag{2.32}$$

Wir betrachten nun eine solche Maschine, die in der Lage sein soll, einen *beliebigen* Zustand zu kopieren, insbesondere die beiden Zustände $|\phi\rangle$ und $|\psi\rangle$. Also

$$\hat{U}(|\phi\rangle \otimes |A\rangle) = |\phi\rangle \otimes |\phi\rangle \,, \tag{2.33}$$
$$\hat{U}(|\psi\rangle \otimes |A\rangle) = |\psi\rangle \otimes |\psi\rangle \,. \tag{2.34}$$

Multipliziert man diese beiden Gleichungen miteinander, erhält man die Bedingung

$$\langle\phi|\,\psi\rangle = (\langle\phi|\,\psi\rangle)^2. \tag{2.35}$$

Diese Gleichung hat genau zwei Lösungen: Entweder ist $\langle\phi|\,\psi\rangle = 1$, was bedeutet, dass die Zustände identisch sind, oder es ist $\langle\phi|\,\psi\rangle = 0$, die Zustände sind also orthogonal. Eine allgemeine Quantenkopiermaschine funktioniert also für unterschiedliche Zustände nur genau dann, wenn alle Zustände orthogonal sind. Dieser Sachverhalt ist als *no-cloning theorem* bekannt: Es ist nicht möglich, einen unbekannten Quantenzustand zu vervielfältigen.

Wir akzeptieren damit, dass es im Fall einer Quantenkommunikation unter Umständen nicht möglich ist, das Ausgangssymbol zu rekonstruieren. Eine obere Schranke für die erhaltbare Information ist dabei die *Holevo-Schranke*:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x). \tag{2.36}$$

Das angegebene Beispiel einer einfachen Quantenkommunikation erweckt den Anschein, als könnten Aufgaben, die mit klassischer Kommunikation trivial einfach sind, bei Verwendung von Quantenzuständen nicht befriedigend vollbracht werden. Wir werden aber sehen, dass – bei geeigneter Ausnutzung von Quanteneigenschaften – genau das Gegenteil der Fall ist.

2.3 Quantenkryptographie

Die Disziplin der Quantenkryptographie entsteht aus einem Zusammenschluss von Quantenmechanik und Informationstheorie. Die Grundideen der Quantenkryptographie wurden zuerst von Charles Bennett und Gilles Brassard Mitte der 1980er Jahre formuliert. Tatsächlich hatte Stephen Wisner bereits in den 70ern ähnliche Konzepte skizziert [Gis02]. Seine revolutionäre Arbeit wurde jedoch erst ein Jahrzehnt später veröffentlicht. Die grundlegenden Möglichkeiten einer Quanteninformationstheorie entspringen dabei erstaunlicherweise nicht aus *zusätzlichen Freiheiten*, die die Quantenmechanik mit sich bringt, sondern aus *zusätzlichen Einschränkungen*. Die folgenden Einschränkungen sind dabei so simpel wie folgenreich:

1 | Es ist *nicht möglich*, an einem quantenmechanischen System eine Messung durchzuführen, ohne das System dabei zu stören.

2 | Es ist *nicht möglich*, den Wert konjugierter Variablen gleichzeitig mit beliebiger Genauigkeit zu messen (Heisenberg-Unschärferelationen).

3 | Es ist *nicht möglich*, einen unbekannten Quantenzustand zu kopieren (*No-cloning Theorem*).

Die erstaunliche Charakteristik der Quanteninformation besteht darin, diese *Einschränkungen* für Anwendungen in einem positiven Sinne nutzbar zu machen.

Die (klassische) Kryptographie befasst sich mit der Problematik, eine geheime Nachricht in eine Form zu bringen, so dass eine unauthorisierte Person nicht in der Lage ist, den Inhalt der Nachricht in Erfahrung zu bringen. Die Kryptographie ist damit eine Unterdisziplin der Kryptologie, die sich zusätzlich mit Kryptoanalyse befasst. Die geheime Nachricht wird zu diesem Zweck mit einem Algorithmus (*cipher*) bearbeitet, der die Nachricht mit weiteren Informationen (dem *Schlüssel*) kombiniert und somit eine verschlüsselte Version der Nachricht (*Kryptogramm*) erzeugt.

Dabei soll sichergestellt werden, dass kein Dritter in der Lage ist, das Kryptogramm unauthorisiert zu entschlüsseln. Es muss also zum einen sichergestellt werden, dass kein Dritter in den Besitz des Schlüssels kommt, zum anderen ist sicherzustellen, dass eine abgehörte Nachricht in keinem Fall *ohne Kenntnis des Schlüssels* entziffert werden kann.

Ein antikes Verschlüsselungsverfahren (bekannt als *„Caesar's cipher"*) beruht zum Beispiel auf einer linearen Verschiebung im Alphabet. Eine Klartextnachricht wird nach dem Schema „A→B, B→C, C→D, ..." kodiert. Natürlich ist die Sicherheit dieses Schlüssels sehr fraglich: Schlichtes Ausprobieren entziffert die Nachricht in Minuten! Ist die Nachricht hinreichend lang, könnte ein Abhörer auch die Häufigkeiten des Auftretens der verschiedenen Buchstaben auswerten und mit der bekannten charakteristischen Statistik der verwendeten Sprache vergleichen. Wie kann aber die Sicherheit eines *ciphers* vergrößert werden?

Die Sicherheit klassischer Kryptographie-Verfahren beruht auf Annahmen über die Leistungsfähigkeit von Computern. Die zu übertragende Nachricht wird verschlüsselt und die vermeintliche Sicherheit resultiert aus der Verwendung sogenannter *one-way functions* $f(x)$ als Schlüssel, bei denen es einfach ist, $f(x)$ aus bekanntem x zu berechnen, aber schwierig, aus bekanntem $f(x)$ auf x zurückzuschließen. Die Worte „einfach" und „schwierig" beziehen sich dabei lediglich auf die Zeit, die ein Computer benötigt, um die entsprechenden Berechnungen durchzuführen. Steigt die benötigte Rechenleistung exponentiell, gilt ein Verfahren als sicher. Steigt sie lediglich polynomial, wird die Sicherheit in Frage gestellt. Alle heute gängigen Verfahren zur Verschlüsselung beruhen auf der Annahme, dass es sich beim *Faktorisieren großer Zahlen* um eine *one-way function* handelt. Demnach ist es einfach, aus gegebenen Primfaktoren die Zahl 67×71 zu berechnen, allerdings dauert es ungleich länger, die Primfaktoren der Zahl 4757 zu bestimmen. Diese Tatsache ist allerdings sofort gefährdet, falls zusätzliche Informationen zur Verfügung stehen. Ist etwa bekannt, dass 67 ein Primfaktor von 4757 ist, wird das Problem der Primfaktorenzerlegung sehr einfach. Ein weiteres Problem dieses Verfahrens besteht darin, dass der mathematische Beweis, dass es sich bei der Faktorisierung tatsächlich um ein „schwieriges Problem" handelt, aussteht. Damit ist nicht ausgeschlossen, dass ein Algorithmus existiert, mit dem das Problem *einfach* wird. Tatsächlich konnte Peter Shor 1994 nachweisen, dass ein Quantencomputer in der Lage ist, das Problem der Faktorzerlegung großer Zahlen in polynomialer Zeit zu erledigen. Gelingt die technologische Realisierung eines Quantencomputers, müssen praktisch alle aktuell verwendeten Verschlüsselungsmethoden ersetzt werden.

Ein leistungsfähiges klassisches Verschlüsselungsverfahren ist der sogenannte *Vernam cipher* (1917). Dabei wird die zu versendende Nachricht zuerst in eine binäre Darstellung gebracht. Als Schlüssel verfügen Sender und Empfänger nun über je eine Kopie einer zufälligen Bitfolge. Der Sender führt eine bitweise Addition von Nachricht und Schlüssel durch, der Empfänger

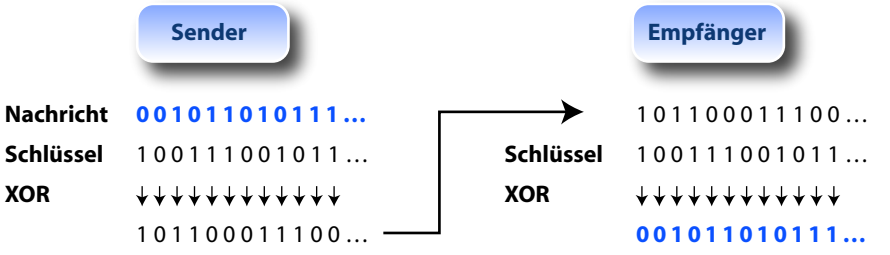

Abbildung 2.5 — Funktionsprinzip des *Vernam ciphers*. Eine binär dargestellte Nachricht wird mittels eines zufälligen binären Schlüssels, über den sowohl Sender als auch Empfänger verfügen müssen, verschlüsselt. Dazu werden Nachricht und Schlüssel bitweise verglichen und gemäß der Vorschrift $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$ kodiert. Die verschlüsselte Nachricht wird übertragen und auf Seiten des Empfängers mit dem gleichen Schlüssel unter Anwendung der gleichen Vorschrift wieder entschlüsselt.

entschlüsselt in der gleichen Weise (⇝Abbildung 2.5).

Unter der Voraussetzung, dass es sich bei dem Schlüssel um eine *rein zufällige* Bitfolge handelt, kann man zeigen, dass der Vernam cipher ein extrem sicheres Mittel zur Verschlüsselung von Nachrichten darstellt. Selbstverständlich gilt dies nur, solange kein Dritter in den Besitz des verwendeten Schlüssels gelangt.

2.3.1 Das BB84 Protokoll

Der Vorteil der Quantenkryptographie besteht nun darin, dass die damit erreichte Sicherheit nicht auf Annahmen über die Leistungsfähigkeit von Rechnern basiert, sondern auf physikalischen Grundlagen. Das erste Quantenkryptographieprotokoll dieser Art wurde von Charles Bennett und Gilles Brassard 1984 vorgestellt [Ben84] und wird gemeinhin als „BB84-Protokoll“ bezeichnet.

Dieses Protokoll löst die Aufgabe, einen geheimen Schlüssel, mit dem im Folgenden eine Nachricht verschlüsselt werden soll (etwa per *Vernam cipher*), von einem Sender zu einem Empfäger zu übertragen, ohne dass diese Schlüsselübertragung (*Quantum Key Distribution* – QKD) mitgehört werden kann. Grundlage des BB84-Protokolls ist die Übertragung des Schlüssels mittels

Gesendete Polarisation	／	／	／	＼	＼	＼	—	—	—	|	|	|
Basis des Empfängers	×	+	+	×	+	+	×	×	+	×	×	+
Gemessene Polarisation	／	—	|	＼	—	|	＼	／	—	＼	／	|
Gleiche Basis?	j	n	n	j	n	n	n	n	j	n	n	j
Schlüssel	1	.	.	0	.	.	.	.	0	.	.	1

Abbildung 2.6 — Zum Funktionsprinzip des BB84-Protokolls. Die Symbole (|), (—), (＼) und (／) bezeichnen die vier möglichen Polarisationen und die Symbole (+) und (×) bezeichnen die beiden Basissysteme, die zur Messung verwendet werden können.

Quantenzuständen, normalerweise einzelnen Photonen. Der zu übertragende Schlüssel wird dabei in die Polarisation der Photonen hineinkodiert. Ein solches Quantensystem, das über zwei Eigenwerte verfügt, wird als *quantum bit* oder *qbit* bezeichnet.

Der Sender präpariert eine Reihe von Photonen und entscheidet sich bei jedem Photon *rein zufällig* für eine von zwei Basen. Hat der Sender sich für eine Basis entschieden, die wir mit (+) bezeichnen, kann er nun ein horizontal (—) oder ein vertikal (|) polarisiertes Photon an den Empfänger übersenden. Hat er sich für die $-45°/+45°$-Basis (×) entschieden, kann er entweder ein Photon senden, welches unter $-45°$ (＼) oder unter $+45°$ (／) polarisiert ist. Da die Wahl der Basis rein zufällig erfolgt, wird jede Wahl statistisch gleich häufig auftreten.

Der Empfänger registriert die bei ihm eingehende Sequenz von Photonen und führt an jedem Photon eine Messung der Polarisation durch. Dabei entscheidet auch er sich bei jeder Messung rein zufällig für eine der beiden Basen (+) oder (×). Es ist sofort klar, dass genau in den Fällen, in denen Sender und Empfänger *zufällig* die gleiche Basis gewählt haben, genau das präparierte Bit auch empfangen wird. Arbeiten Sender und Empfänger in unterschiedlicher Basis, so erhält der Empfänger in der Hälfte der Fälle das falsche Bit. Nach dem Ende der Übertragung verständigen sich Sender und Empfänger darüber, in welchen Fällen sie dieselbe Basis verwendet haben (es werden *nicht* die Resultate verglichen!). Die Fälle unterschiedlicher Basis werden schlicht ignoriert. Nun kann man auch den gemessenen Polarisationen Bitwerte 0 und 1 zuweisen und hat auf diesem Wege einen Schlüssel übertragen, der nun zur Verschlüsselung und Entschlüsselung einer echten Nachricht bei beiden Parteien vorliegt.

Der Vorteil einer solchen Quantenschlüsselübertragung wird klar, wenn

man bedenkt, dass die Schlüsselübertragung abgehört werden könnte. Dies könnte dadurch geschehen, dass ein Mithörer jedes übertragene Photon abfängt und in einer zufällig gewählten Basis vermisst. Das gemessene Ergebnis wird dann vom Abhörer zum Empfänger weitergeschickt. Denkbar sind dabei zwei Fälle:

1 | Der Mithörer misst zufällig in der richtigen Basis. In diesem Fall kennt der Mithörer das übertragene Bit, Sender und Empfänger sind ahnungslos.

2 | Der Mithörer misst in der falschen Basis (Hälfte der Fälle). In diesem Fall wird durch die Messung der Quantenzustand verändert und der ursprüngliche Empfänger wird wiederum in der Hälfte der Fälle ein falsches Bit erhalten.

Nach dem Übertragen des Schlüssels führen also Sender und Empfänger eine Überprüfung durch. Dazu wählen sie einen Teil der übertragenen Bits aus und vergleichen. Offenbart sich dabei eine Fehlerquote von 25%, so wissen beide, dass mitgehört wurde. Der übertragene Schlüssel wird in diesem Fall verworfen. Man beachte, dass der Mithörer in jedem Fall eine Messung an dem übertragenen Photon durchführen muss. Das Anfertigen und Vermessen einer Kopie ist wegen des *no-cloning-theorems* nicht möglich.

Jeder reale Übertragungskanal kann nicht störungsfrei sein, was bedeutet, dass man eine gewisse Fehlerquote auch dann erwarten muss, wenn kein Mithörer die Übertragung gestört hat. Dies ist jedoch keine prinzipielle Begrenzung des Verfahrens, sondern ein rein technisches Problem, welches mittels Fehlerkorrekturverfahren und Hash-Funktionen (teilweise oder ganz) behoben werden kann.

2.3.2 Dense Coding

Die Möglichkeiten, die ein Quanteninformationsprotokoll gegenüber klassischen Protokollen auszeichnen, werden besonders deutlich, wenn man ein Verfahren betrachtet, das als *Dense Coding* bekannt geworden ist [Ben92]. Dieses Verfahren basiert auf der Annahme, dass Sender und Empfänger sich die Teilsysteme eines verschränkten Zustandes teilen. Die Präparation und Verteilung des verschränkten Paares ist dabei nicht Bestandteil des Protokolls. Wir betrachten den verschränkten Zustand

$$|\phi\rangle = (|0\rangle_S |0\rangle_E + |1\rangle_S |1\rangle_E). \tag{2.37}$$

Die Indizes S und E unterscheiden dabei die Teile des Zustandes, über die Sender bzw. Empfänger verfügen. Der Sender hat nun die Freiheit, an seinem Teil des Zustandes eine von insgesamt vier Operationen vorzunehmen:

1 | Es wird nichts unternommen, der Zustand bleibt unverändert.

2 | Durchführung eines *bit-flip*. Dieser bewirkt $|0\rangle \rightarrow |1\rangle$ oder $|1\rangle \rightarrow |0\rangle$.

3 | Durchführung eines *phase-flip*. Dieser bewirkt, dass der Zustand $|0\rangle$ unverändert bleibt, aber $|1\rangle \rightarrow -|1\rangle$.

4 | Durchführung eines *bit-flip und eines phase-flip*.

Nach der Manipulation wird der Zustand dem Empfänger zugestellt, der nun also einen Gesamtzustand in einem der vier Zustände

$$|a\rangle = \left|\phi^+\right\rangle = (|0\rangle_S |0\rangle_E + |1\rangle_S |1\rangle_E) \quad \text{oder} \tag{2.38}$$
$$|b\rangle = \left|\psi^+\right\rangle = (|1\rangle_S |0\rangle_E + |0\rangle_S |1\rangle_E) \quad \text{oder} \tag{2.39}$$
$$|c\rangle = \left|\phi^-\right\rangle = (|0\rangle_S |0\rangle_E - |1\rangle_S |1\rangle_E) \quad \text{oder} \tag{2.40}$$
$$|d\rangle = \left|\psi^-\right\rangle = (|1\rangle_S |0\rangle_E - |0\rangle_S |1\rangle_E) \tag{2.41}$$

hat. Diese vier Zustände sind alle paarweise orthogonal, was bedeutet, dass der Empfänger eine Messung durchführen kann, die in der Lage ist, die vier Zustände zu unterscheiden. Der Empfänger verfügt nunmehr also über einen Zustand, der zwei Bit Informationen enthält, obwohl der Sender lediglich ein Bit über den Kommunikationskanal übertragen hat. Genau dieser Effekt – der kein klassisches Analogon besitzt – wird als *Dense Coding* bezeichnet.

2.3.3 Quantenteleportation

Wir betrachten ganz ähnlich wie beim Dense Coding den Fall, dass sich Sender und Empfänger ein verschränktes Paar teilen

$$|\phi\rangle = (|0\rangle_S |0\rangle_E + |1\rangle_S |1\rangle_E). \tag{2.42}$$

Darüber hinaus verfügt der Sender über einen beliebigen Quantenzustand

$$|\kappa\iota\rho\kappa\rangle = \mu |0\rangle_S + \nu |1\rangle_S \tag{2.43}$$

ohne diesen Quantenzustand genau zu kennen. Wir betrachten den Gesamtzustand:

$$|\Psi\rangle = (\mu |0\rangle_S + \nu |1\rangle_S)(|0\rangle_S |0\rangle_E + |1\rangle_S |1\rangle_E). \tag{2.44}$$

Ausmultiplizieren und Umstellen führt auf die folgende Darstellung:

$$\begin{aligned}|\Psi\rangle \;=\; & (|0\rangle_S|0\rangle_S + |1\rangle_S|1\rangle_S)(\mu|0\rangle_E + \nu|1\rangle_E) \\ & +(|0\rangle_S|0\rangle_S - |1\rangle_S|1\rangle_S)(\mu|0\rangle_E - \nu|1\rangle_E) \\ & +(|0\rangle_S|1\rangle_S + |1\rangle_S|0\rangle_S)(\mu|1\rangle_E + \nu|0\rangle_E) \\ & +(|0\rangle_S|1\rangle_S - |1\rangle_S|0\rangle_S)(\mu|0\rangle_E - \nu|1\rangle_E). \end{aligned} \tag{2.45}$$

Der Sender kann an seinem Teil des Zustandes nun eine Messung vornehmen und dabei lernen, welcher der vier Zustände $|\phi^+\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$ auf seiner Seite vorliegt. Abhängig vom Ergebnis dieser Messung teilt der Sender dem Empfänger nun per *klassischer Kommunikation* mit, was dieser mit seinem Teil des Zustandes tun soll: Hat der Sender den Zustand $|\phi^+\rangle$ gemessen, lautet die Anweisung „Nichts unternehmen!“. Wurde der Zustand $|\phi^-\rangle$ vorgefunden, wird dem Empfänger mitgeteilt, er solle einen *phase-flip* durchführen. Im Fall $|\psi^+\rangle$ wird ein *bit-flip* benötigt. Letztlich soll im Fall $|\psi^-\rangle$ sowohl ein *phase-flip*, als auch ein *bit-flip* durchgeführt werden.

Im Resultat hat der Empfänger unter Benutzung zweier Bits klassischer Information eine exakte Kopie vom unbekannten Zustand $|\kappa\iota\rho\kappa\rangle$ des Senders hergestellt. Der unbekannte Quantenzustand ist somit *teleportiert* worden. Man mache sich klar, dass dieses Verfahren keine Quantenkopiermaschine ist: Der Ausgangszustand ist auf Seiten des Senders bei der Projektionsmessung zerstört worden.

2.3.4 Kontinuierliche Variablen

Praktisch alle Konzepte einer quantenbasierten Informationstheorie sind auf Basis diskreter Zustände (qbits) entwickelt worden. Diese historische Tatsache ist logisch, da im Fall solcher diskreter Zustände intuitive Vorstellungen über Informationstheorie unmittelbar übertragbar sind. Denkt man allerdings über experimentelle Realisierungen dieser Überlegungen nach, so sind gerade kontinuierliche Systeme besonders attraktiv. Dabei wird die zu bearbeitende Information in den Wert kontinuierlicher Variablen (CVs) eines Zustandes hineinkodiert. Es bietet sich an, zu diesem Zweck zum Beispiel Amplitude und Phase eines elektromagentischen (Licht-)Feldes zu verwenden.

Die dann zum Tragen kommenden Vorteile liegen auf der Hand: Im Gegensatz zu (realen) diskreten Systemen sind solche kontinuierlichen Systeme vergleichsweise einfach zu generieren, zu manipulieren und mit großer Geschwindigkeit und hoher Effizienz zu detektieren. Vor dem Hintergrund einer

technologischen Implementierung ist vor allem die hohe Detektionsgeschwindigkeit (entsprechend einer hohen Übertragungsrate) zu sehen. Vergleichbare Detektoren stehen im Regime diskreter Variablen nicht zur Verfügung.

Zwischenzeitlich sind im Regime kontinuierlicher Variablen sehr erfolgreich Quantenkommunikationsprotokolle experimentell implementiert worden. Als wichtigste sind zu nennen: Quantenteleportation [Fur98], Quantum Key Distribution [Hir03][Gro03], Quantum Secret Sharing [Lan04], Quantum Erasing [And04] und Entanglement Swapping [Jia04].

2.4 Schlussfolgerung

Wir hatten bei der Betrachtung einiger Quanteninformationsstrategien gesehen, dass dabei die Übertragung von Quantenzuständen zwischen räumlich getrennten Parteien („Sender“ und „Empfänger“) stattfindet. Einerseits tragen dabei die transportierten Zustände selber Information und sind damit Bestandteil des Protokolls. Wir hatten aber auch insbesondere gesehen, dass verschiedene Informationsprotokolle darauf basieren, dass sich die beteiligten Parteien die Konstituenten eines verschränkten Paares teilen. In jedem realistischen Szenario würde diese Verteilung von Quantenzuständen durch einen störungsbehafteten Kanal erfolgen (Übertragung durch Luft oder per optischer Faser). Im Fall einer solchen Übertragung sind durch Störvorgänge die nichtklassischen Eigenschaften der übertragenen Zustände gefährdet.

In der klassischen Nachrichtentechnik werden gegen die Störeffekte des Kanals (Verringerung des Signal/Rausch-Verhältnisses, Phasenverschiebungen, Verzerrungen der Signalform) sogenannte *repeater* eingesetzt, die in der Lage sind, die Signalstärke zu erhöhen und gegebenenfalls die Signalform zu korrigieren oder Signale zu resynchronisieren.

Die verläßliche Übertragung von Quanteninformation über einen optischen Kanal ist das Hauptproblem bei jeder realistischen Umsetzung eines Quanteninformationsprotokolls, da Störeffekte des Kanals exponentiell mit der Länge desselben skalieren. Da nun Quantenzustände nicht vervielfältigt werden können (*no-cloning theorem*), ist es nicht möglich, ein einfaches Analogon zu einem klassischen Repeater zu konstruieren.

Stattdessen muss man die Sichtweise korrigieren: Statt den Anspruch zu erheben, einen unbekannten (und zum Beispiel verschränkten) Zustand über einen langen optischen Kanal zu *transportieren*, ohne dass die Stärke der Verschränkung darunter leidet, genügt es, zwischen zwei Parteien einen maximal

verschränkten Zustand zu *etablieren*. Dieser Wechsel der Perspektive ist die Grundlage einer Destillation von Quantenzuständen. Die in der vorliegenden Arbeit durchgeführte Demonstration von Destillation und Purifikation gequetschter Zustände demonstriert genau die Umsetzung dieser Idee.

KAPITEL 3

Nichtklassisches Licht

3.1 Feldquantisierung

Die Quantennatur des Lichtes spielt für die vorliegende Arbeit eine entscheidende – nämlich absolut grundlegende – Rolle. Aus diesem Grund ist es notwendig, ein solides Verständnis für die quantenartigen Eigenschaften des Lichtes zu entwickeln. Es ist also sinnvoll, die Ableitung dieser Eigenschaften ausführlich darzustellen. In meiner Darstellung folge ich [Ger05].

Ausgangspunkt der Überlegungen sind die Maxwell-Gleichungen. Wir betrachten ein monochromatisches elektromagnetisches Feld, welches sich in z-Richtung ausbreiten soll. Nimmt man weiterhin an, dass die elektrische Komponente dieses Feldes in x-Richtung polarisiert sein soll, erhält man die bekannten Lösungen der Maxwell-Gleichungen (in SI-Einheiten):

$$E_x(z,t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} q(t)\sin(kz) \tag{3.1}$$

und für das magnetische Feld, das dann in y-Richtung polarisiert ist:

$$B_y(z,t) = \left(\frac{\mu_0\epsilon_0}{k}\right)\left(\frac{2\omega^2}{V\epsilon_0}\right) p(t)\cos(kz). \tag{3.2}$$

In diesen Gleichungen sind k die Wellenzahl, $q(t)$ ein zeitabhängender Faktor mit der Dimension einer Länge und $p(t) = \dot{q}(t)$ ein zeitabhängender Faktor mit der Dimension einer Geschwindigkeit. Die Vorfaktoren hängen

natürlich vom verwendeten Einheitensystem ab und sollen hier nicht weiter interessieren. Als Hamiltonfunktion dieses Feldes erhält man:

$$H(q,p) = \frac{1}{2}(p^2 + \omega^2 q^2). \tag{3.3}$$

Die Ähnlichkeit zur Hamiltonfunktion des klassischen harmonischen Oszillators kann nicht übersehen werden. Um den Übergang zur quantenmechanischen Beschreibung dieses Systems zu machen, wird nun einfach die Ersetzungsregel angewendet, man ersetzt also jede kanonische Variable durch einen entsprechenden Operator:

$$q \to \hat{q}, \quad p \to \hat{p} \quad \text{mit} \quad [\hat{q},\hat{p}] = i\hbar. \tag{3.4}$$

Unter Anwendung dieser Ersetzungsregeln erhält man nun Operatoren für das elektrische und magnetische Feld ($\hat{E}_x$ und $\hat{B}_y$), sowie den Hamiltonoperator

$$\hat{H} = \frac{1}{2}(\hat{p}^2 + \omega^2 \hat{q}^2). \tag{3.5}$$

Es ist nun hilfreich, aus den Operatoren $\hat{q}$ und $\hat{p}$ zwei (zunächst willkürliche) neue Operatoren in der Form

$$\hat{a} = (2\hbar\omega)^{-1/2}(\omega\hat{q} + i\hat{p}) \quad \text{und} \tag{3.6}$$

$$\hat{a}^\dagger = (2\hbar\omega)^{-1/2}(\omega\hat{q} - i\hat{p}) \tag{3.7}$$

zu kombinieren. Diese neuen Operatoren sind – anders als $\hat{q}$ und $\hat{p}$ – nicht hermitesch und korrespondieren daher nicht mit Observablen. Bei $\hat{a}$ und $\hat{a}^\dagger$ handelt es sich natürlich um die bekannten (bosonischen) Vernichter- und Erzeugeroperatoren des elektromagnetischen Feldes mit der wichtigen Kommutatorrelation

$$[\hat{a},\hat{a}^\dagger] = 1, \tag{3.8}$$

aus der wir mehrfach Nutzen ziehen werden. Mit diesen Operatoren schreibt sich der Hamiltonoperator in der nützlichen Form

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{3.9}$$

Man will nun auswerten, welche Aussagen über die Energie eines solchen Zustandes in diesem Hamiltonoperator enthalten sind. Dazu bezeichnen wir mit $|n\rangle$ einen Eigenzustand des Hamiltonoperators ⇝Gleichung (3.9), der zu

einem Energieeigenwert E_n gehört. Man kann somit eine Eigenwertgleichung für diesen Zustand $|n\rangle$ aufschreiben:

$$\hat{H}\,|n\rangle = E_n\,|n\rangle\,. \tag{3.10}$$

Diese Gleichung entspricht lediglich der Aussage, dass $|n\rangle$ ein Eigenzustand des Hamiltonoperators zum Eigenwert E_n sein soll. Multipliziert man dies von links mit $\hat{a}^\dagger$, erhält man eine neue Eigenwertgleichung

$$\hbar\omega\left(\hat{a}^\dagger\hat{a}^\dagger\hat{a} + \frac{1}{2}\hat{a}^\dagger\right)|n\rangle = E_n\hat{a}^\dagger\,|n\rangle\,. \tag{3.11}$$

Um diese umzuformen benutzt man nun die Kommutatorrelation ⇝Gleichung (3.8) zwischen Vernichter und Erzeuger und kann damit umschreiben:

$$\hat{H}(\hat{a}^\dagger\,|n\rangle) = (E_n + \hbar\omega)(\hat{a}^\dagger\,|n\rangle). \tag{3.12}$$

Hierbei handelt es sich wiederum um eine Eigenwertgleichung, diesmal für den Zustand $\hat{a}^\dagger\,|n\rangle$, der offenbar erstens ebenfalls ein Eigenzustand des Hamiltonoperators ist und zweitens den Eigenwert $E_n + \hbar\omega$ besitzt. Damit ist die Begriffsbildung des Erzeugeroperators klar geworden, denn seine Anwendung erzeugt offenbar ein Quant der Energie $\hbar\omega$. Führt man die Rechnung analog für den Operator $\hat{a}$ durch, erhält man als Ergebnis, dass zu einem Zustand $\hat{a}\,|n\rangle$ der Eigenwert $E_n - \hbar\omega$ gehört. Dieser Operator vernichtet also ein Quant mit Energie $\hbar\omega$. Da die Gesamtenergie des Feldes nicht negativ werden darf, muss es einen Zustand minimaler Energie geben, den wir *Grundzustand* oder *Vakuumzustand* nennen und mit dem Symbol $|0\rangle$ bezeichnen. Wir erklären die Wirkung des Vernichteroperators auf diesen Zustand durch:

$$\hat{a}\,|0\rangle = 0. \tag{3.13}$$

Die Eigenwertgleichung für den Vakuumzustand schreibt sich

$$\hat{H}\,|0\rangle = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|0\rangle = \frac{1}{2}\hbar\omega\,|0\rangle\,, \tag{3.14}$$

woran man ablesen kann, dass dieser Zustand minimaler Energie *nicht* Energie $E_0 = 0$ hat, sondern über eine Nullpunktsenergie $\hbar\omega/2$ verfügt. Da wir nun wissen, dass jede Anwendung des Erzeugeroperators ein Quant der Energie $\hbar\omega$ erzeugt, kann man die Energieeigenwerte des Hamiltonoperators vom Grundzustand ausgehend konstruieren und aufschreiben:

$$E_n = \hbar\omega\left(n + \frac{1}{2}\right). \tag{3.15}$$

Hieran liest man durch Vergleich mit dem Hamiltonoperator ⇝Gleichung (3.9) ab, dass für die Wirkung des *Anzahloperators* $\hat{n} = \hat{a}^\dagger \hat{a}$ auf einen Zustand $|n\rangle$ gilt:

$$\hat{n}\,|n\rangle = n\,|n\rangle\,. \tag{3.16}$$

Die Anwendung des Anzahloperators läßt also den Zustand unverändert und liefert als Eigenwert die Anzahl der Quantenanregungen (gemessen in Vielfachen von $\hbar\omega$) zurück. Nachdem wir bisher die Wirkung des Vernichteroperators explizit nur für den Vakuumzustand erklärt hatten, berechnen wir nun die Wirkung des Vernichters auf einen beliebigen Zustand $|n\rangle$. Wir wissen, dass der Vernichteroperator die Anregung des Zustandes um ein Quant $\hbar\omega$ vermindert:

$$\hat{a}\,|n\rangle = c_n\,|n-1\rangle\,. \tag{3.17}$$

Zur Bestimmung der Konstanten c_n berechnen wir das Skalarprodukt des Zustandes $\hat{a}\,|n\rangle$ mit sich selbst:

$$\begin{aligned}(\langle n|\,\hat{a}^\dagger)(\hat{a}\,|n\rangle) &= \langle n|\,\hat{a}^\dagger\hat{a}\,|n\rangle = n &(3.18)\\ &= \langle n-1|\,c_n^* c_n\,|n-1\rangle = |c_n|^2. &(3.19)\end{aligned}$$

Damit haben wir $c_n = \sqrt{n}$. Für den Erzeuger rechnet man analog. Zusammenfassend haben wir gefunden:

$$\begin{aligned}\hat{a}\,|n\rangle &= \sqrt{n}\,|n-1\rangle\,, &(3.20)\\ \hat{a}^\dagger\,|n\rangle &= \sqrt{n+1}\,|n+1\rangle\,, &(3.21)\\ \hat{a}^\dagger\hat{a}\,|n\rangle &= n\,|n\rangle\,. &(3.22)\end{aligned}$$

Nimmt man diese Ergebisse zusammen, kann man einen beliebigen Zustand $|n\rangle$ erhalten, indem man wiederholt den Erzeuger auf den Grundzustand $|0\rangle$ anwendet. Inklusive Normierung kann man schreiben:

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle\,. \tag{3.23}$$

Die Zustände aus ⇝Gleichung (3.23) nennt man *Photonenzahl-* oder *Fockzustände*. Sie spielen bei der Beschreibung von Einzelphotonexperimenten eine Rolle.

3.1.1 Quantenfluktuationen

Wie wir im vorangegangenen Abschnitt gesehen haben, hat der Zustand $|n\rangle$ im monochromatischen Fall eine wohldefinierte Energie $E_n = (n + 1/2)\hbar\omega$.

Die Energie eines Zustandes ist aber in quantenoptischen Experimenten keine Observable, die einer unmittelbaren Messung zugänglich ist. Vielmehr verwendet man als Messgerät Photodetektoren, die das elektrische Feld, bzw. das Quadrat desselben messen. Dabei ist weiterhin zu bedenken, dass typische Photodetektoren eine geringe Bandbreite aufweisen, verglichen mit der optischen Frequenz ω des elektrischen Feldes. Die zeitliche Variation des Feldes bei der optischen Frequenz ω wird also nicht zeitaufgelöst registriert – es findet ein Mittelungsprozess statt. Wir betrachten nun das elektrische Feld, welches zu einem Fockzustand gehört. Wir werden zu dem zunächst überraschenden Ergebnis kommen, dass das elektrische Feld keinen wohldefinierten Wert haben wird. Zwar verschwindet für Fockzustände die mittlere Feldstärke

$$\langle n|\, \hat{E}_x(z,t)\, |n\rangle = \mathcal{E}_0 \sin(kz)[\langle n|\, \hat{a}\, |n\rangle + \langle n|\, \hat{a}^\dagger\, |n\rangle] = 0, \tag{3.24}$$

weil $\langle n|\, m\rangle = \delta^n_m$ (die Fockzustände sind orthogonal), nicht jedoch das Mittel der Quadrate, also die mittlere Feldenergie:

$$\langle n|\, \hat{E}_x^2(z,t)\, |n\rangle = 2\mathcal{E}_0^2 \sin^2(kz) \left(n + \frac{1}{2}\right), \tag{3.25}$$

wobei wir im Faktor $\mathcal{E}_0$ aus Bequemlichkeit die Konstanten absorbiert haben. Berechnet man nun aus ⇝Gleichung (3.24) und ⇝Gleichung (3.25) die Varianz des elektrischen Feldes, indem man

$$\Delta^2 \hat{O} = \langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2 \tag{3.26}$$

verwendet (die Durchführung dieser Rechnung bleibt dem Leser überlassen), sieht man, dass selbst im Grundzustand $n = 0$ diese Varianz nicht verschwindet. Wird ein solches Feld mit einem geeigneten Detektor vermessen, so streuen die Messwerte mit dieser Varianz um einen Mittelwert. Man mache sich klar, dass dieser Effekt nicht aus einer Schwäche des Messprozesses resultiert (ein solcher ist bisher nicht explizit betrachtet worden), sondern eine Eigenschaft des vermessenen Zustandes ist: Bei dieser Streuung handelt es sich um die Vakuumfluktuationen des elektrischen Feldes.

3.1.2 Quadraturoperatoren

Wir führen nun die Quadraturoperatoren ein, die zu einer äußerst nützlichen Anschauung von Zuständen im Phasenraum führen werden. Diese Darstellung ermöglicht es, eine umfangreiche Intuition bezüglich des Verhaltens quantenoptischer Lichtzustände zu entwickeln. Ausgehend von Erzeuger und

Vernichter definiert man (wiederum zunächst willkürlich erscheinend) einen neuen hermiteschen Operator $\hat{X}^\theta$, der vom *Quadraturwinkel* θ parametrisiert wird:

$$\hat{X}^\theta = \hat{a}e^{-i\theta} + \hat{a}^\dagger e^{i\theta}. \tag{3.27}$$

(Die Hermitezität weist man nach, indem man die Kommutatorrelation von Erzeuger und Vernichter ausnutzt.) Bewertet man diesen Operator für zwei Quadraturwinkel $\theta = 0$ und $\theta = \pi/2$, so erhält man die Operatoren der Amplituden- und Phasenquadratur, die mit $\hat{X}^+$ (Amplitude) und $\hat{X}^-$ (Phase) bezeichnet werden:

$$\hat{X}^{\theta=0} =: \hat{X}^+ = \hat{a} + \hat{a}^\dagger, \tag{3.28}$$

$$\hat{X}^{\theta=\pi/2} =: \hat{X}^- = -i(\hat{a} - \hat{a}^\dagger). \tag{3.29}$$

In Umkehrung kann man aus diesen beiden Operatoren wiederum den Operator einer beliebigen Quadratur als Linearkombination darstellen:

$$\hat{X}^\theta = \hat{X}^+ \cos(\theta) + \hat{X}^- \sin(\theta). \tag{3.30}$$

Mit Hilfe der beiden Operatoren $\hat{X}^+$ und $\hat{X}^-$ schreibt man das elektrische Feld

$$\hat{E}_x(z,t) \propto \sin(kz)[\hat{X}^+ \cos(\omega t) + \hat{X}^- \sin(\omega t)]. \tag{3.31}$$

In dieser Darstellung wird die Bezeichnung als Quadraturoperatoren klar, denn offenbar korrespondieren die Operatoren mit Feldamplituden, die eine gegenseitige Phase von 90 Grad besitzen. (Die gängigen Bezeichnungen sind hier leicht unpräzise. Streng genommen bezeichnet man den gesamten Ausdruck $\hat{X}^+ \cos(\theta)$ als *Amplitudenquadratur*. Damit sollte eigentlich $\hat{X}^+$ die Bezeichnung *Amplitudenquadraturamplitude* tragen. Entsprechend sollte $\hat{X}^-$ als *Phasenquadraturamplitude* bezeichnet werden. Diese umständlichen Benennungen haben sich aber nicht durchgesetzt und sind zu *Amplitudenquadratur* und *Phasenquadratur*, manchmal sogar schlicht zu *Amplitude* und *Phase* verkürzt worden. Mit dieser Ungenauigkeit kann man leben, sofern man ihren Ursprung kennt und Verwirrung vermeidet.) Unter Ausnutzung der bekannten Kommutatorrelationen für Erzeuger- und Vernichteroperator berechnet man leicht den Kommutator für die Quadraturoperatoren:

$$[\hat{X}^+, \hat{X}^-] = 2i \tag{3.32}$$

Die Tatsache, dass dieser Kommutator nicht verschwindet, ist gleichbedeutend mit der Existenz einer Unschärferelation zwischen den beiden Operatoren. Man kann allgemein zeigen, dass für zwei Operatoren, deren Kommutator

nicht verschwindet $[\hat{O}_1, \hat{O}_2] = \alpha$ eine Unschärfebeziehung $\Delta\hat{O}_1\Delta\hat{O}_2 \geq 1/2\alpha$ folgt.

$$\Delta\hat{X}^+\Delta\hat{X}^- \geq 1. \tag{3.33}$$

Für einen Zustand $|n\rangle$ gilt zwar

$$\langle n|\,\hat{X}^+\,|n\rangle = \langle n|\,\hat{X}^-\,|n\rangle = 0, \tag{3.34}$$

aber

$$\begin{aligned}
\langle n|\,\hat{X}^+\hat{X}^+\,|n\rangle &= \langle n|\,\hat{a}^2 + \hat{a}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\,|n\rangle && (3.35)\\
&= \langle n|\,\hat{a}^2 + \hat{a}^\dagger\hat{a}^\dagger + 2\hat{a}^\dagger\hat{a} + 1\,|n\rangle && (3.36)\\
&= (2n+1) && (3.37)
\end{aligned}$$

und entsprechend für $\hat{X}^-$. Berechnet man aus diesen Audrücken wiederum die Varianz, findet man, dass für einen solchen Zustand die Fluktuationen der beiden Quadraturen gleich groß sind. Außerdem sieht man sofort ein, dass ein Vakuumzustand das Unschärfeprodukt minimiert.

3.2 Kohärente Zustände

Wir hatten die Anzahl- oder Fockzustände $|n\rangle$ eingeführt. Unser Ziel ist jedoch eine Beschreibung quantenoptischer Experimente, die Laserstrahlen verwenden mit Leistungen in der Größenordnung von einem Watt. Bei den dabei auftretenden extrem großen Anregungen stellen die Fockzustände kein sinnvolles Werkzeug zur Beschreibung mehr dar. Es wird häufig ausgeführt, dass man zum klassischen Grenzfall gelangt, wenn man einen solchen Fockzustand für eine sehr große Anregung (also eine große Photonanzahl n) betrachtet und damit n für alle praktischen Belange die Eigenschaften einer kontinuierlichen Variablen annimmt. Wir hatten jedoch gezeigt, dass der Erwartungswert des elektrischen Feldes in einem Fockzustand stets verschwindet: $\langle n|\,E_x\,|n\rangle = 0$. Dies gilt insbesondere auch, wenn n sehr groß wird. Aus der klassischen Vorstellung wissen wir jedoch, dass das elektrische Feld an einem festen Ort sinusförmig oszilliert. Um einen Zustand zu erhalten, der diesen Sachverhalt besser darstellt, betrachten wir Eigenzustände des Vernichteroperators

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{3.38}$$

Der Eigenwert α kann in diesem Fall zunächst komplex sein, da $\hat{a}$ kein hermitescher Operator ist. Wir entwickeln den Zustand $|\alpha\rangle$ in der Basis der Fockzustände:

$$|\alpha\rangle = \sum_{n=0}^{\infty} C_n |n\rangle . \tag{3.39}$$

Dies können wir als Ansatz in die Eigenwertgleichung einsetzen und erhalten

$$\hat{a} |\alpha\rangle = \sum_{n=0}^{\infty} C_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} C_n |n\rangle . \tag{3.40}$$

Ein Koeffizientenvergleich führt auf

$$C_n = \frac{\alpha}{\sqrt{n}} C_{n-1} = \frac{\alpha^2}{\sqrt{n(n-1)}} C_{n-2} = \ldots \tag{3.41}$$

$$= \frac{\alpha^n}{\sqrt{n!}} C_0. \tag{3.42}$$

Damit schreibt sich der Zustand als

$$|\alpha\rangle = C_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{3.43}$$

Die Konstante C_0 bestimmt man aus der Normierungsbedingung $\langle \alpha | \alpha \rangle = 1$ und erhält schließlich

$$|\alpha\rangle = \exp(-\frac{1}{2}|\alpha|^2) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{3.44}$$

Für diesen *kohärenten Zustand* läßt sich nun zeigen, dass der Erwartungswert des elektrischen Feldes nicht verschwindet, sondern wie im klassischen Fall eine sinusförmige Oszillation ausführt. Wir haben damit eine Darstellung gefunden, die alle Vorstellungen von einem Laserstrahl wiedergibt. Unter Verwendung der Quadraturoperatoren kann man außerdem zeigen, dass für die Varianzen gilt

$$\Delta^2 \hat{X}^{+/-} = 1, \tag{3.45}$$

der kohärente Zustand hat also für alle Anregungen α Fluktuationen, die in ihrer Varianz genau dem Vakuumrauschen entsprechen (das ist bei Fockzuständen nicht der Fall!).

Wir betrachten zuletzt erneut den Anzahloperator $\hat{n}$. Für die mittlere Photonenzahl eines Zustandes $|\alpha\rangle$ ergibt sich:

$$n = \langle\alpha|\,\hat{n}\,|\alpha\rangle = |\alpha|^2. \tag{3.46}$$

Um die Fluktuationen der Photonenanzahl zu erhalten, benötigen wir noch den Erwartungswert von $\hat{n}^2$:

$$\begin{aligned} \langle\alpha|\,\hat{n}^2\,|\alpha\rangle &= \langle\alpha|\,\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}\,|\alpha\rangle & (3.47)\\ &= |\alpha|^4 + |\alpha|^2 = n^2 + n. & (3.48) \end{aligned}$$

und damit

$$\Delta^2 n = \left\langle\hat{n}^2\right\rangle - \langle\hat{n}\rangle^2 = n, \tag{3.49}$$

was charakteristisch für einen Poisson-Prozess ist.

Wir hatten eben den kohärenten Zustand als Eigenzustand des Vernichteroperators erhalten. Dies ist nicht die einzige Möglichkeit, diese Darstellung zu erhalten. Eine weitere Möglichkeit, einen kohärenten Zustand zu definieren, besteht in der Einführung des sogenannten (unitären) Displacement-Operators $\hat{D}$, der gegeben ist als

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}). \tag{3.50}$$

Einen kohärenten Zustand erhält man dann, indem man den Displacement-Operator (der die kohärente Anregung α als Parameter enthält) auf den Vakuumzustand anwendet:

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle = \exp(-1/2|\alpha|^2)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{3.51}$$

was identisch mit dem kohärenten Zustand ⇝Gleichung (3.44) ist.

3.3 Gequetschte Zustände

Es ist aus den Grundlagen der Quantenmechanik bekannt (und nicht schwer zu zeigen), dass wenn für zwei Operatoren $\hat{A}$ und $\hat{B}$ eine Kommutatorrelation $[\hat{A},\hat{B}] = \alpha$ gilt, für die Varianzen folgt

$$(\Delta^2\hat{A})(\Delta^2\hat{B}) \geq \frac{1}{4}|\alpha|^2. \tag{3.52}$$

Dies ist die allgemeine Darstellung einer Heisenberg-Unschärferelation. Sind die beiden Varianzen $\Delta^2\hat{A}$ und $\Delta^2\hat{B}$ gleich groß und ist gleichzeitig in der Gleichung der Fall der Gleichheit gegeben, spricht man von einem *Zustand minimaler Unschärfe* oder *minimum uncertainty state* (MUS). Wir gehen nun von einer allgemeinen Definition aus: Ein Zustand heißt *gequetscht*, wenn

$$\Delta^2\hat{A} < \frac{1}{2}|\alpha| \quad \text{oder} \quad \Delta^2\hat{B} < \frac{1}{2}|\alpha|. \tag{3.53}$$

Wegen der ersten Gleichung (⇝Gleichung (3.52)) können jedenfalls nicht beide Varianzen kleiner sein als $1/2|\alpha|$. Wir spezialisieren dies nun, indem wir als Operatoren den Amplituden- und Phasenoperator herannehmen. Mit der Kommutatorrelation für diese Operatoren heißt ein Zustand des elektromagnetischen Feldes gequetscht, wenn

$$\Delta^2\hat{X}^+ < 1 \quad \text{oder} \quad \Delta^2\hat{X}^- < 1. \tag{3.54}$$

Für einen kohärenten Zustand hatten wir $\Delta^2\hat{X}^+ = \Delta^2\hat{X}^- = 1$ gefunden. Ein Zustand, für den eine der Bedingungen (⇝Gleichung (3.54)) gilt, besitzt also in der entsprechenden Quadratur eine Varianz, die geringer ist als die Varianz des Vakuumrauschens. Offenbar muss dabei die Varianz der entsprechend orthogonalen Quadratur vergrößert werden, um nicht die Unschärfebeziehung zu verletzen. Die Erzeugung eines solchen Zustandes gelingt mathematisch mit Hilfe des (unitären) Squeezingoperators, der durch

$$\hat{S}(\xi) = \exp\left(\frac{1}{2}(\xi^*\hat{a}^2 - \xi\hat{a}^\dagger\hat{a}^\dagger)\right) \tag{3.55}$$

gegeben ist. Dabei setzt man zur Abkürzung

$$\xi = re^{i\phi}. \tag{3.56}$$

In diesem Ausdruck ist r der sogenannte Squeezingparameter $0 < r < \infty$ und ϕ eine Phase mit $0 < \phi < 2\pi$. Es wird beim Betrachten klar, dass dieser Operator eine Art Zwei-Photonen-Korrelation erwirkt, da Photonen von ihm paarweise erzeugt oder vernichtet werden. (Die Existenz eines solchen Operators motiviert auch die Einführung des Verschiebeoperators im Abschnitt über kohärente Zustände. Zusammen mit weiteren Operatoren (etwa Zeitentwicklungsoperator und Phasenverschiebungsoperator) erhält man eine ganze Sammlung unitärer Operatoren, mit deren Hilfe bequem Zustände

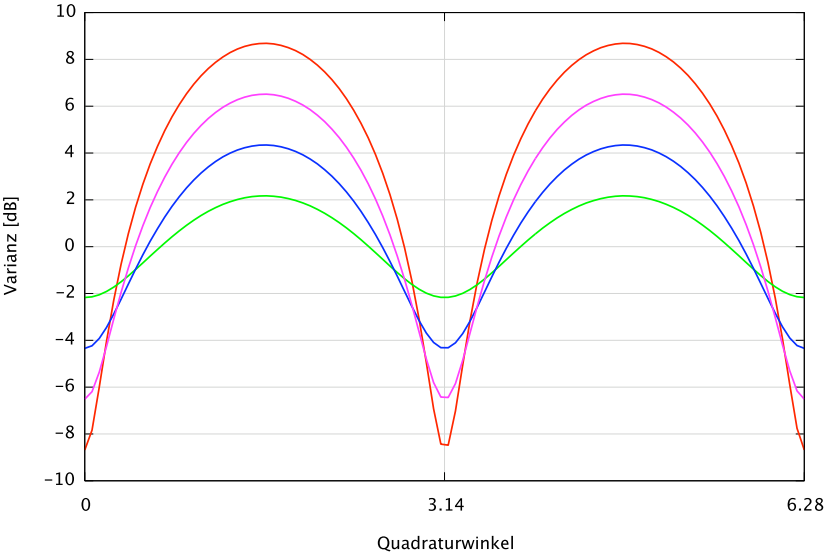

Abbildung 3.1 — Darstellung des Squeezings über dem Quadraturwinkel bei einem Zustand, der in der Amplitudenquadratur gequetscht ist. Die Phasenquadratur ($\theta = \pi/2$) ist folglich antigequetscht. An der Darstellung auf einer logarithmischen dB-Achse kann man unmittelbar ablesen, wie die Gültigkeit der Unschärfebeziehung sichergestellt wird. Dargestellt sind vier verschiedene gequetschte Zustände für unterschiedliche Squeezingparameter ($r = 0{,}25$ (grün), $r = 0{,}5$ (blau), $r = 0{,}75$ (pink), $r = 1$ (rot)).

manipuliert werden können). Wir wollen die Wirkung des Operators $\hat{S}$ auf einen Zustand betrachten:

$$|s\rangle = \hat{S}\,|\psi\rangle\,. \tag{3.57}$$

Um die Varianzen der Quadraturoperatoren zu berechnen, benötigt man die Erwartungswerte von Erzeuger und Vernichter im gequetschten Zustand. Man kann zunächst für den Squeezingoperator die beiden folgenden Ausdrücke aufschreiben, die wir verwenden wollen:

$$\hat{S}^\dagger \hat{a} \hat{S} = \hat{a}\cosh(r) - \hat{a}^\dagger e^{i\phi}\sinh(r), \tag{3.58}$$

$$\hat{S}^\dagger \hat{a}^\dagger \hat{S} = \hat{a}^\dagger\cosh(r) - \hat{a}e^{-i\phi}\sinh(r). \tag{3.59}$$

Für den Fall eines Vakuumzustandes erhält man damit für die Varianzen

$$\Delta^2\hat{X}^+ = \cosh^2(r) + \sinh^2(r) - 2\sinh(r)\cosh(r)\cos(\phi), \tag{3.60}$$

$$\Delta^2\hat{X}^- = \cosh^2(r) + \sinh^2(r) + 2\sinh(r)\cosh(r)\cos(\phi). \tag{3.61}$$

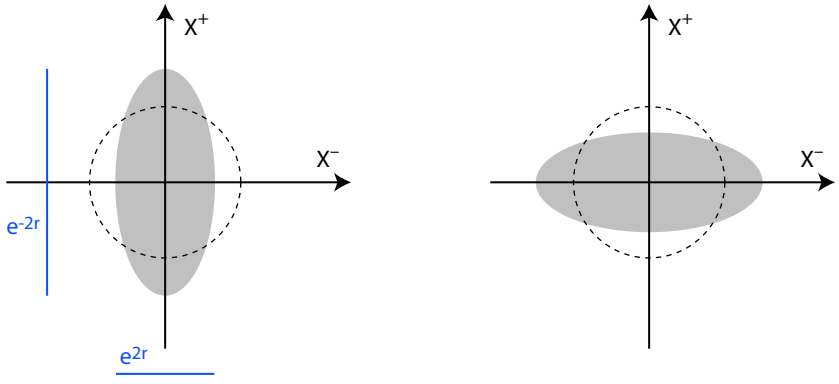

Abbildung 3.2 — Darstellung eines phasen- und eines amplitudengequetschten Vakuumzustandes im Quadraturraum (Phasenraum). Kreis bzw. Ellipsenkontur repräsentieren eine Höhenlinienkontur der Verteilungsfunktion von Messwerten.

Im Fall $\phi = 0$ reduzieren sich diese Ausdrücke zu

$$\Delta^2 \hat{X}^+ = \exp(-2r) \quad \text{und} \tag{3.62}$$
$$\Delta^2 \hat{X}^- = \exp(2r). \tag{3.63}$$

Es ist offensichtlich, dass in diesem Fall ($\phi = 0$) die $\hat{X}^+$-Quadratur gequetscht ist. Für eine andere Wahl ($\phi = \pi$) wäre die $\hat{X}^-$-Quadratur gequetscht. Man beachte, dass die jeweils andere Quadratur eine vergrößerte Varianz aufweist, um die Gültigkeit der Unschärfebeziehung sicherzustellen. Diese Quadratur vergrößerter Varianz wird häufig auch als „anti-gequetschte Quadratur" bezeichnet. Weiterhin erkennt man, dass für diese Varianzen die Unschärfebeziehung minimiert wird (Zustand minimaler Unschärfe, MUS). Es ist weder notwendig, noch im Allgemeinen gegeben, dass gequetschte Zustände die Unschärfebeziehung minimieren.

Eine nützliche Möglichkeit der Veranschaulichung gequetschter Zustände ist die Phasenraumrepräsentation. Zwei Darstellungen mit Squeezing in der $\hat{X}^+$- und $\hat{X}^-$-Quadratur sind in der ⇝Abbildung 3.2 illustriert. Dies entspricht den Fällen $\phi = 0$ und $\phi = \pi$. Für eine andere Wahl von ϕ ist es sinnvoll, rotierte Quadraturoperatoren $\hat{Y}^+$ und $\hat{Y}^-$ einzuführen:

$$\begin{pmatrix} \hat{Y}^+ \\ \hat{Y}^- \end{pmatrix} = \begin{pmatrix} \cos(\phi/2) & \sin(\phi/2) \\ -\sin(\phi/2) & \cos(\phi/2) \end{pmatrix} \begin{pmatrix} \hat{X}^+ \\ \hat{X}^- \end{pmatrix}. \tag{3.64}$$

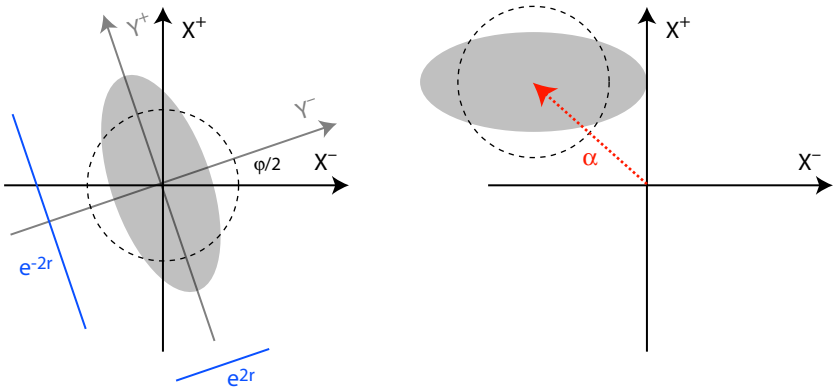

Abbildung 3.3 — Darstellung eines Zustandes, der entlang einer beliebigen Quadratur gequetscht ist. Rechts: Darstellung eines amplitudengequetschten Zustandes mit kohärenter Anregung α.

Auch für diese Operatoren kann man wiederum leicht zeigen, dass

$$\Delta^2\hat{Y}^+ = \exp(-2r) \quad \text{und} \tag{3.65}$$
$$\Delta^2\hat{Y}^- = \exp(2r) \tag{3.66}$$

gilt. Das Squeezing und Antisqueezing ist also nicht auf die Amplituden- oder Phasenquadratur beschränkt, sondern kann entlang beliebiger orthogonaler Quadraturen vorliegen. Zu einer weiteren Verallgemeinerung gelangt man, wenn man auf einen beliebig gequetschten Vakuumzustand den Displacementoperator anwendet:

$$|\alpha, \xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)\,|0\rangle\,. \tag{3.67}$$

Die Reihenfolge der Anwendungen von Squeezing- und Displacementoperator kann im Prinzip auch umgekehrt werden, was auf einen von Yuen [Yue76] eingeführten Zustand führt. Man rechnet leicht nach, dass für einen solchen Zustand gilt:

$$\langle\alpha, \xi|\,\hat{n}\,|\alpha, \xi\rangle = |\alpha|^2 + \sinh^2(r). \tag{3.68}$$

Hieran liest man ab, dass beim Quetschen eines Zustandes Photonen erzeugt werden, denn der Erwartungswert des Anzahloperators $\hat{n}$ wird um einen Beitrag $\sinh^2(r)$ vergrößert. Auch im Fall eines solchen Zustandes mit kohärenter

Anregung findet man

$$\Delta^2\hat{Y}^+ = \exp(-2r), \tag{3.69}$$
$$\Delta^2\hat{Y}^- = \exp(2r). \tag{3.70}$$

Die Charakteristik des Quantenrauschens wird also durch die kohärente Anregung α eines Zustandes nicht beeinflusst.

3.4 Wigner-Funktion

Die Wigner-Funktion ist ein nützliches Werkzeug zur Darstellung klassischer und nichtklassischer Zustände des Lichtes. Im Jahr 1932 führte Eugene Wigner, der das Ziel hatte, die Wellenfunktion durch eine Wahrscheinlichkeitsverteilung im Phasenraum zu ersetzen die sogenannte Wigner-Wahrscheinlichkeitsverteilung ein [Wig32].

Man denke an einen klassischen harmonischen Oszillator. Seine Zeitentwicklung wird durch einen Punkt im Phasenraum (aufgespannt von einer Ortskoordinate X und einer Impulskoordinate P) vollständig definiert. Für eine sehr große Anzahl solcher Oszillatoren kann man eine Wahrscheinlichkeitsverteilung als Funktion $W(X,P)$ angeben, die die Wahrscheinlichkeit bezeichnet, ein Teilchen an den Koordinaten (X,P) vorzufinden. Eine solche Verteilung muss positiv und normiert sein.

Misst man lediglich eine Koordinate (etwa X) des Oszillators immer wieder, erhält man eine Marginalverteilung $\mathrm{pr}(X)$. Diese hängt mit der Wignerverteilung zusammen:

$$\mathrm{pr}(X) = \int W(X,P)dP. \tag{3.71}$$

Macht man nun den Übergang zur Quantenmechanik, so macht die Vorstellung eines Punktes im Phasenraum keinen Sinn mehr, denn die beiden Phasenraumkoordinaten können nur limitiert durch eine Heisenberg-Unschärfe simultan gemessen werden. Dennoch kann man eine der Variablen sehr oft vermessen und erhält wiederum eine Marginalverteilung. Diese sollte nun wieder eine Projektion einer Quasiwahrscheinlichkeitsdichte – der *Wignerfunktion* – sein. Die Wignerfunktion eines gegebenen Zustandes erhält man etwa aus der Dichtematrix.

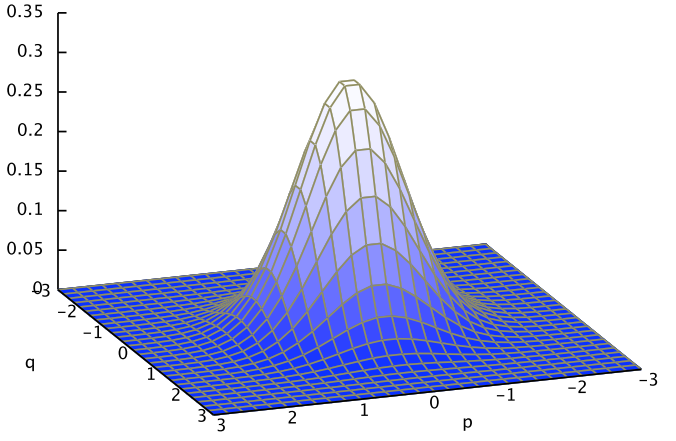

Abbildung 3.4 — Wignerfunktion des Vakuumzustandes $|0\rangle$. Die Unschärfescheibe kann erkannt werden, wenn man sich eine Kartenprojektion der Wignerfunktion in die x-y-Ebene vorstellt und eine beliebige Kontur auszeichnet.

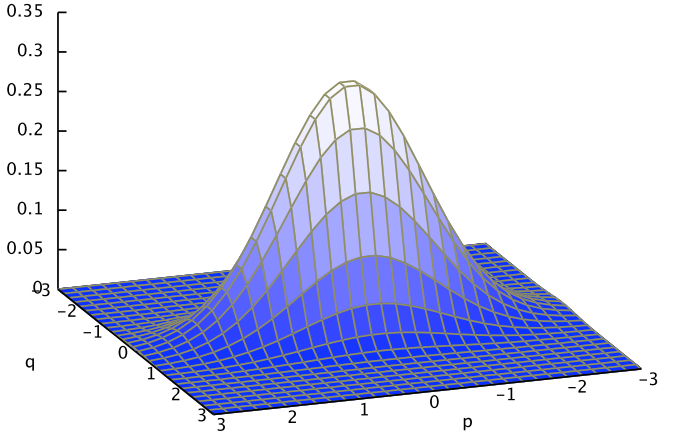

Abbildung 3.5 — Wignerfunktion eines gequetschten Vakuumzustandes mit 3 dB Squeezing. Eine Projektion führt auf die Squeezing-Ellipse.

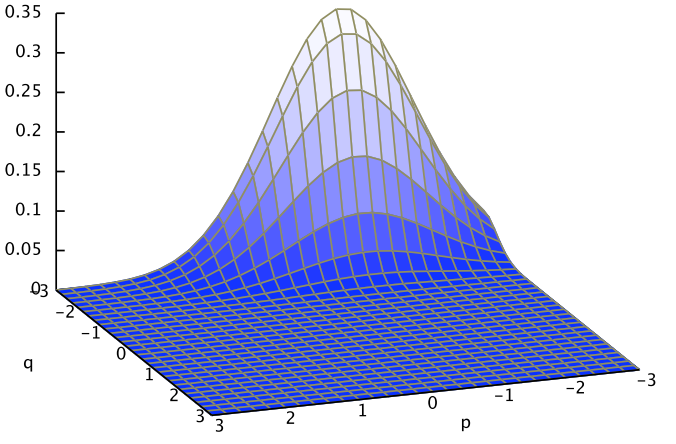

Abbildung 3.6 — Wignerfunktion eines verschobenen gequetschten Vakuumzustandes. Eine Projektion ergibt die Squeezing-Ellipse

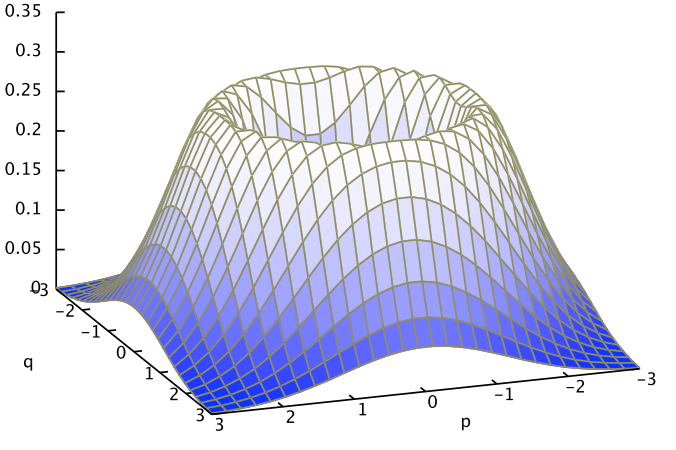

Abbildung 3.7 — Wignerfunktion eines Photonenzahlzustandes mit genau einem Photon, also $|1\rangle$.

Man illustriert den Nutzen der Wignerfunktion, indem man für einen kohärenten Zustand explizit vorrechnet. Ausgangspunkt ist jeweils die Wignergleichung:

$$W(q,p) = \frac{1}{2\pi}\int e^{ipx}\left\langle q-\frac{x}{2}\right|\hat{\rho}\left|q+\frac{x}{2}\right\rangle dx, \tag{3.72}$$

wobei $\hat{\rho}$ die Dichtematrix des Zustandes ist:

$$\hat{\rho} = |\Psi\rangle\langle\Psi|. \tag{3.73}$$

Die Wellenfunktion eines kohärenten Zustandes ist gegeben durch

$$|\Psi\rangle = \pi^{1/4}\exp\left(-\frac{q^2}{2}\right). \tag{3.74}$$

Setzt man die Definition der Dichtematrix in die Wignergleichung ein, erhält man

$$W(q,p) = \frac{1}{2\pi}\int e^{ipx}\left\langle q-\frac{x}{2}\right|\Psi\left\rangle\right\langle\Psi\left|q+\frac{x}{2}\right\rangle dx. \tag{3.75}$$

Einsetzen der Wellenfunktion und umformen führt direkt zum Ziel:

$$\begin{aligned} W(q,p) &= \frac{1}{2\pi}\int dx\pi^{-1/2}\exp\left(-\frac{(q-x/2)^2}{2}-\frac{(q+x/2)^2}{2}\right)e^{ipx} \\ &= \frac{1}{2\pi}\pi^{-1/2}\int dx\exp\left(-\frac{2q^2}{w}-\frac{x^2}{4}+ipx\right) \\ &= \frac{1}{\pi}\exp\left(-q^2-p^2\right). \end{aligned} \tag{3.76}$$

Die Ausführungen und Berechnungen zu Wigner-Funktionen werden in diesem Abschnitt nicht zum Selbstzweck betrieben. Für das Verständnis der Dinge, die bei der Purifikation und Destillation von gequetschten Zuständen des Lichtes eine Rolle spielen, sind die Wignerfunktionen vielmehr ein hervorragendes Hilfsmittel, um die Intuition zu schulen und die Anschauung zu fördern. Dazu macht man sich klar, dass die Wignerfunktionen eine Aussage über die Wahrscheinlichkeitsverteilung von Punkten im Phasenraum machen. Betrachtet man nun etwa die Wignerfunktion eines Vakuumzustandes, so kann man sofort ablesen, dass beim Vermessen eines solchen Zustandes mit der größten Wahrscheinlichkeit der Messwert $(p,q) = (0,0)$ erhalten wird. Weniger wahrscheinlich ist der Wert $(p,q) = (1,0)$, noch seltener kommt $(p,q) = (1,1)$ vor. In einem späteren Abschnitt werden wir den Umgang mit dieser Vorstellung perfektionieren.

3.5 Erzeugung gequetscher Zustände

3.5.1 Bemerkungen zur Historie

Als erstes und grundlegendes Experiment zur Erzeugung von gequetschtem Licht wird gemeinhin die Arbeit von Slusher [Slu85] angesehen. Die Geschichte nichtklassischer Zustände reicht jedoch wesentlich weiter in die Vergangenheit zurück. Verfolgt man die historische Entwicklung zurück [Dod02], so findet man drei grundlegende Arbeiten von Schrödinger [Sch26], Kennard [Ken27] und Darwin [Dar27], die sich mit der Zeitentwicklung eines gaußschen Wellenpaketes, einem freien Teilchen und einem Teilchen im konstanten elektromagnetischen Feld befassen. Die dort beschriebenen Zustände können als Prototypen der gequetschten und kohärenten Zustände angesehen werden. Damit sind diese Zustände zwischenzeitlich rund 80 Jahre lang bekannt.

Die erste detallierte Betrachtung eines gequetschten Zustandes erfolgte durch Yuen [Yue76], der die Bezeichnung *Zweiphotonen-Zustand* verwendete. Später fanden die Begriffe *squeezing* und *squeezed states* allgemeine Verwendung – sie wurden erstmals in den Veröffentlichungen von Hollenhorst [Hol79] und Caves [Cav81] verwendet. Die beiden genannten Artikel befassen sich erstaunlicherweise mit den Grundlagen des interferometrischen Nachweises von Gravitationswellen – ein Umstand, der den engen Bezug zwischen der Entwicklung von gequetschten Zuständen und der Gravitationswellenforschung treffend zum Ausdruck bringt.

Eine (subjektive!) Auswahl von 74 wichtigen Experimenten aus dem Bereich der Erzeugung gequetschter Zustände mittels unterschiedlicher Verfahren kann man in ⇝Abbildung 3.8 und ⇝Abbildung 3.9 betrachten.

3.5.2 Verfahren

Für die experimentelle Erzeugung gequetscher Zustände sind eine Reihe von Verfahren bekannt und erprobt worden (siehe ⇝Abbildung 3.8 und ⇝Abbildung 3.9). Diese Verfahren können hier nicht im Detail beschrieben werden (einen guten und detaillierten Überblick findet man zum Beispiel in [Bac04]). Wichtige Prozesse und Strategien, die bezüglich der Erzeugung gequetschter Zustände betrachtet werden müssen, sind:

1 | Vierwellen-Mischung. Diese Verfahren wurde von Slusher [Slu85] im ersten Squeezing-Experiment verwendet. Ein Atomstrahl wird mit Laserlicht gepumpt. Ein zweiter Strahl passiert die Atome und wird per

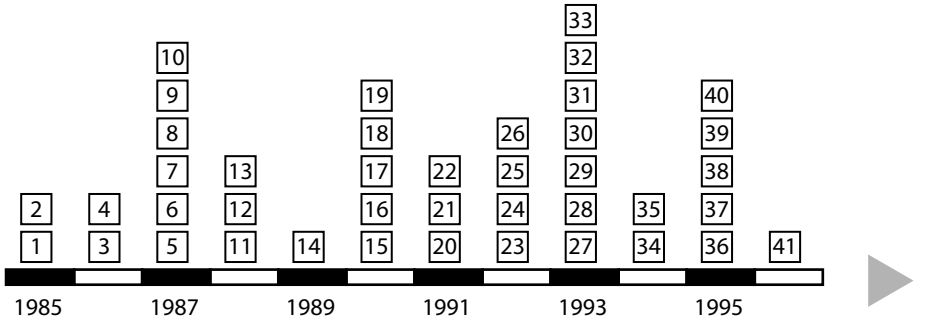

Abbildung 3.8 — Timeline wichtiger Squeezing-Experimente, Teil1. 1: Slusher, PRL **55**, 2409 2: Levenson, Opt. Lett. 10, 514 3: Wu, PRL **57**, 2520 4: Shelby, PRL **57**, 691 5: Slusher, PRL **59**, 2566 6: Grangier, PRL **59**, 2153 7: Xiao, PRL **59**, 278 8: Raizen, PRL **59**, 198 9: Schumaker, PRL **58**, 357 10: Wu, J. Opt. Soc. Am. B4, 1465 11: Pereira, PRA **38**, 4931 12: Machida, PRL **60**, 792 13: Yurke, PRL **60**, 764 14: Yurke, PRA **39**, 2519 15: Movshovich, PRL **65**, 1419 16: Nabors, PRA **42**, 556 17: Kumar, PRL **64**, 1015 18: Richardson, PRL **64**, 400 19: Sizmann, Opt. Commun. 80, 138 20: Richardson, PRL **66**, 2867 21: Rosenbluh, PRL **66**, 153 22: Bergmann, Opt. Lett. 16, 663 23: Hope, PRA **46**, R1181 24: Polzik, PRL **68**, 3020 25: Townsend, PRA **45**, 458 26: Polzik, Appl. Phys. B 55, 279 27: Wang, PRL **71**, 3951 28: Roch, PRL **71**, 2006 29: Inoue, PRA **48**, 2230 30: Koashi, PRL **71**, 1164 31: Ou, PRL **70**, 3239 32: Smithey, PRl **70**, 1244 33: Kürz, Europhys. Lett. 24, 449 34: Kim, PRL **73**, 1605 35: Paschotta, PRL **72**, 3807 36: Kitching, PRL **74**, 3372 37: Fox, PRL **74**, 1728 38: Ralph, Opt. Lett. 20, 1316 39: Tsuchida, Opt. Lett. 20, 2240 40: Breitenbach, J. Opt. Soc. Am. B12, 2304 41: Friberg, PRL **77**, 3775

Heterodyndetektion vermessen. Der Vierwellen-Mischprozess kann als phasensensitiver Verstärkungsprozess angesehen werden (Verstärkung der Amplitudenquadratur bei gleichzeitiger Abschwächung der Phasenquadratur).

2 | Second Harmonic Generation (SHG). Basiert auf der Nichtlinearität $\chi^{(2)}$ bestimmter optischer Kristalle. Bei der Frequenzverdopplung wird ein Photonenpaar einer fundamentalen Wellenlänge in ein einzelnes Photon der doppelten Frequenz umgesetzt. Die Wahrscheinlichkeit für das Stattfinden dieses Prozesses ist über die Nichtlinearität mit der Intensität der fundamentalen Mode gekoppelt. Die fundamentale Welle trägt Quantenrauschen. Führt dies in einem Moment zu einem größeren Wert der Feldstärke, findet die Umsetzung in die zweite Harmonische *wahr-*

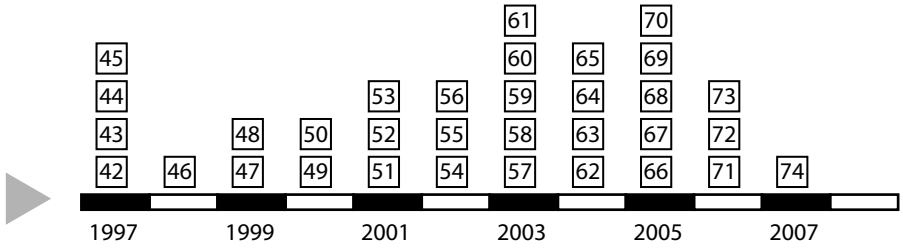

Abbildung 3.9 — Timeline wichtiger Squeezing-Experimente, Teil 2. 42: Bruckmeier, **79**, 43 43: Kilper, PRA **55**, R3323 44: Li, PRL **78**, 3105 45: Bruckmeier, PRL **78**, 1243 46: Schmitt, PRL **81**, 2446 47: Li, PRL **82**, 5225 48: Lam, J. Opt. B: Quantum Semiclass. Opt. **1**, 469 49: Daly, PRA **62**, 043807 50: Zhang, PRA **62**, 023813 51: Zhang, PRA **64**, 033815 52: Fiorentino, PRA **64**, 031801 53: Silberhorn, PRL **86**, 4267 54: McKenzie, PRL **88**, 231102 55: Bowen, PRL **88**, 093601 56: Buchler, PRA **65**, 011803 57: Ries, PRA **68**, 025801 58: Heersink, PRA **68**, 013815 59: Jing, PRL **90**, 167903 60: Zhang, PRA **67**, 033802 61: Bowen, PRL **90**, 043601 62: Laurat, PRA **70**, 042315 63: McKenzie, PRL **93**, 161105 64: Wenger, PRL **92**, 153601 65: Karr, PRA **69**, 031802 66: Vahlbruch, PRL **95**, 211102 67: Takei, PRA **72**, 042304 68: Hirosawa, PRL **94**, 203601 69: Chelkowski, PRA **71**, 013806 70: Mizuno, PRA **71**, 012304 71: Jing, PRA **74**, 041804 72: Franzen, PRL **97**, 150505 73: Vahlbruch, PRL **97**, 011101 74: Chelkowski, PRA **75**, 043814

scheinlicher statt, als im nächsten Moment eines vom Quantenrauschen verursachten kleineren Wertes. Auf diesem Wege wird die Messstatistik sowohl der fundamentalen als auch der frequenzverdoppelten Mode verändert, was zu Squeezing führt.

3 | Kerr-Effekt. Als Kerr-Effekt bezeichnet man eine intensitätsabhängende Phasenverschiebung, wie sie in nichtlinearen Medien (deren Brechungsindex n von der Intensität abhängt) auftritt. In der Phasenraumdarstellung sieht man sofort ein, dass dadurch die „Rauschfläche“ eines kohärenten Zustandes mit Anregung zu einer Ellipse, bzw. einer bananenförmigen Fläche verzerrt wird.

4 | Atome im Resonator. Eine Atomwolke zeigt nichtlineares Verhalten. Da die beteiligten Nichtlinearitäten extrem klein sind, wird die Atomwolke im Innern eines Resonators untergebracht, um die resonante Überhö-

hung der Intensität zu nutzen. Die Anregung der Atome hängt vom Feld im Innern des Resonators ab. Die optische Länge des Resonators wiederum wird durch die Anregung der Atome beeinflusst. Auf diesem Weg wird eine Korrelation zwischen der Amplituden- und Phasenquadratur des Feldes geschaffen, die zu Squeezing führt.

5 | Optische Pulse. Verwendet man gepulste Laser, so können leicht extrem hohe Intensitäten und damit nichtlineare Wechselwirkungen erzielt werden. Es ist daher nicht überraschend, dass lange Zeit mit gepulsten Laserquellen die besten Squeezing-Resultate erzielt werden konnten. Zur Erzeugung von Squeezing kann etwa der Kerr-Effekt in einer optischen Faser verwendet werden. Es sind auch SHG/OPO-Experimente durchgeführt worden, die allerdings bezüglich der Strärke des erreichten Squeezings hinter den Erwartungen weit zurückblieben.

6 | Diodenlaser. Die trivialste Strategie zur Erzeugung von amplitudengequetschtem Laserlicht direkt im Laserprozess. Dazu wird eine Laserdiode mit einem Strom gepumpt, der bereits eine entsprechende Zählstatistik aufweist. Einen solchen Pumpstrom bereit zu stellen ist unproblematisch. Das Problem entsteht bei der Umsetzung dieses Pumpstroms in Photonen. Weicht die Quanteneffizienz der verwendeten Laserdiode von Eins ab, so wird die Statistik nachteilig beeinflusst.

7 | Optisch parametrische Prozesse. Die erfolgreichsten Squeezing-Experimente basieren auf einem optisch parametrischen Prozess (OPO oder OPA) im Innern eines nichtlinearen Kristalls. Man kann zeigen, dass ein solcher Prozess einem rauschfreien phasensensitiven Verstärker entspricht, der also eine Quadratur des Lichtfeldes um einem Faktor (*gain*) verstärkt und dabei die orthogonale Quadratur um *denselben Faktor* abschwächt. Um die Intensität und damit den Effekt der Nichtlinearität zu vergrößern, werden solche Kristalle oft im Innern von optischen Resonatoren angewendet.

3.5.3 Optisch parametrische Prozesse

Viele Verfahren zur Erzeugung gequetschten Lichtes beruhen auf einem parametrischen Effekt in nichtlinearen Medien. Dies gilt auch für die im Rahmen dieser Arbeit erzeugten und verwendeten gequetschten Zustände, die durch parametrische Abwärtskonversion erzeugt wurden. Dabei wird ein nichtlinearer Kristall mit einem starken Feld der Frequenz ω_p gepumpt. Man stellt

sich nun vor, dass einige Photonen dieses Feldes in zwei Photonen identischer Frequenz $\omega = \omega_p/2$ konvertiert werden. Der Hamiltonoperator eines solchen Prozesses kann geschrieben werden als [Ger05]

$$\hat{H} = \hbar\omega\hat{a}^\dagger\hat{a} + \hbar\omega_p\hat{b}^\dagger\hat{b} + i\hbar\chi^{(2)}(\hat{a}\hat{a}\hat{b}^\dagger - \hat{a}^\dagger\hat{a}^\dagger\hat{b}), \tag{3.77}$$

wobei $\hat{b}$ das Pumpfeld und $\hat{a}$ das *Signalfeld* bei der halben Frequenz bezeichnen. Der Term $\chi^{(2)}$ beschreibt die Stärke der Nichtlinearität des koppelnden Mediums. Man nimmt nun an, dass die Pumpmode durch ein klassisches Feld beschrieben werden kann. Diese Annahme ist gerechtfertigt, falls die Pumpmode viel größere Leistung aufweist als das entstehende Signalfeld. Dann kann man ansetzen, dass die Pumpmode durch den parametrischen Prozess nicht nennenswert abgeschwächt wird. Wir nehmen zusätzlich an, dass sich die Pumpmode in einem kohärenten Zustand befindet. Schreibt man die Zeitentwicklung mit auf, lautet dieser Zustand $\left|\beta e^{-i\omega_p t}\right\rangle$.

In der klassischen Näherung ersetzen wir $\hat{b}$ durch $\beta e^{-i\omega_p t}$ und $\hat{b}^\dagger$ durch $\beta^* e^{i\omega_p t}$. Näherungsweise kann man den Hamiltonoperator dann schreiben als

$$\hat{H} = \hbar\omega\hat{a}^\dagger\hat{a} + i\hbar\chi^{(2)}(\beta^*\hat{a}\hat{a}e^{i\omega_p t} - \beta\hat{a}^\dagger\hat{a}^\dagger e^{-i\omega_p t}). \tag{3.78}$$

Betrachtet man nun die Wechselwirkung zwischen den beiden Moden, erhält man den zeitabhängenden Hamiltonoperator

$$\hat{H} = i\hbar\chi^{(2)}(\beta^*\hat{a}\hat{a}e^{i(\omega_p-2\omega)t} - \beta\hat{a}^\dagger\hat{a}^\dagger e^{-i(\omega_p-2\omega)t}), \tag{3.79}$$

der sich vereinfacht, wenn man nun verwendet, dass die Frequenz des Pumpfeldes der doppelten Frequenz des Signalfeldes entsprechen soll:

$$\hat{H} = i\hbar\chi^{(2)}(\beta^*\hat{a}\hat{a} - \beta\hat{a}^\dagger\hat{a}^\dagger). \tag{3.80}$$

Der zugehörende Entwicklungsoperator lautet dann

$$\hat{U} = \exp\left(-\frac{i}{\hbar}\hat{H}t\right) = \exp(\beta^*\hat{a}\hat{a} - \beta\hat{a}^\dagger\hat{a}^\dagger) \tag{3.81}$$

und hat offenbar die gleiche Form, wie der vorher angegebene Squeezingoperator $\hat{S}$. Damit ist klar, dass durch einen solchen Prozess das Quetschen von Licht bewerkstelligt werden kann.

3.5.4 Nichtlineare Kristalle

Es gibt eine Reihe kristalliner Materialen, die eine nennenswerte Nichtlinearität aufweisen und damit prinzipiell zur Erzeugung gequetschter Zustände verwendet werden können. Abhängig von der Anwendung ist man dabei an einem hohen $\chi^{(2)}$ (OPO/OPA und SHG) oder einem hohen $\chi^{(3)}$ (Kerr-Effekt, Vierwellen-Mischung) interessiert. Eine Rolle bei der Wahl des Materials spielen neben der Größe der Nichtlinearität vor allem die Transparenz bei der geplanten Wellenlänge und die Stärke der Doppelbrechung, die man für die Phasenanpassung ausnutzen kann. Mangelnde Transparenz (bzw. hohe lineare Absorption) wirkt im Fall gequetschter Zustände vor allem als Verlustkanal, der die Stärke des Squeezings limitiert. Außerdem führt eine hohe Absorption zur Erwärmung des Kristalls. Damit wird zum einen die Temperaturstabilisierung (Phasenanpassung) erschwert, zum anderen können thermische Linsen auftreten.

Manche Materialien können sich unerwünscht unter hohen Bestrahlungsstärken verändern (*gray tracking*, *green induced infrared absorption* bzw. *blue induced infrared absorption*, *photodarkening*). Das Aufbringen optischer Schichten (hochreflektierend oder antireflektierend) gelingt bei verschiedenen Materialien unterschiedlich gut. Angesichts dieser zahlreichen Eigenschaften überrascht es nicht, dass eine Vielzahl von Materialen erprobt worden sind. Die Herstellung geeigneter Kristalle ist nach wie vor Gegenstand aktueller Forschung. Die am häufigsten verwendeten nichtlinearen Kristalle werden kurz in der Übersicht behandelt:

1 | Über generell hohe Nichtlinearitäten verfügen Lithiumniobat ($LiNbO_3$) und Lithiumtantalat ($LiTaO_3$). Beide Materialen sind in kongruenter und stöchiometrischer Form erhältlich. Die beiden Materialen werden häufig periodisch gepolt und dann als PPLN im Fall des Niobats und als PPLT im Fall des Tantalats bezeichnet (bzw. als PPSLN und PPSTN im Fall der stöchiometrischen Variante). Beide Materialen weisen eine relativ niedrige Zerstörschwelle auf, was mit dem Anspruch hoher Lichtintensitäten konkurriert. Allerdings kann die Zerstörschwelle durch Dotierung mit MgO erheblich heraufgesetzt werden. Die stöchiometrischen Varianten besitzen von vorn herein eine etwas höhere Zerstörschwelle.

2 | Kaliumniobat ($KNbO_3$) weist ebenfalls eine hohe Nichtlinearität auf und wird oft zur Frequenzverdopplung in den blauen Spektralbereich hinein angewendet.

3 | Kristalle aus der Kaliumtitanylphosphat-Familie ($KTiOPO_4$ = KTP) kommen ebenfalls oft zum Einsatz und können erfolgreich periodisch gepolt werden. Weitere Materialen aus dieser Familie umfassen KTA ($KTiOAsO_4$), RTP ($RbTiOPO_4$) und RTA ($RbTiAsPO_4$).

4 | Kaliumdihydrogenphosphat (KH_2PO_4 = KDP) und Kaliumdideuteriumphosphat (KD*P, KD_2PO_4) können mit großen Abmessungen bei gleichzeitig guter optischer Homogenität hergestellt werden. Allerdings sind sie leicht hygroskopisch und weisen keine große Nichtlinearität auf.

5 | Es gibt eine Reihe von Boraten, die sich als nichtlineare optische Kristalle eignen, Lithiumtriborat (LiB_3O_5 = LBO), Cäsiumlithiumborat (CLBO, $CsLiB_6O_{10}$), beta-Bariumborat (β-BaB_2O_4 = BBO), BiB_3O_6 = BIBO und Cäsiumborat (CsB_3O_5 = CBO). Weniger gebräuchlich sind Strontiumberylliumborat ($Sr_2Be_2B_2O_7$ = SBBO), Yttriumcalciumoxyborat (YCOB) und $K_2Al_2B_2O_7$ = KAB.

6 | Weit in den UV-Bereich hinein reichen die Transparenzfenster von Zinkgermaniumdiphosphid ($ZnGeP_2$ = ZGP), Silbergalliumsulfanid ($AgGaS_2$) und Cadmiumselenid (CdSe).

Im Rahmen dieser Arbeit wird die optisch parametrische Verstärkung (OPA) in MgO:$LiNbO_3$ zur Erzeugung gequetschter Zustände verwendet. Das verwendete Gerät wird ebenfalls als OPA bezeichnet. Ein solcher OPA besteht aus einem nichtlinearen Kristall im Innern eines optischen Resonators. Er konvertiert eine einfallende Laserwelle (Pumpe) der Frequenz ω_p in zwei Wellen, die als Signal- und Idlerwellen bezeichnet werden und deren Frequenzen ω_s und ω_i kleiner sind als ω_p. Aus Energieerhaltungsgründen muss offenbar

$$\omega_p = \omega_s + \omega_i \tag{3.82}$$

sein. Für die Erzeugung gequetscher Zustände wird der OPA entartet betrieben, das heißt

$$\omega_i = \omega_s = \omega_p/2. \tag{3.83}$$

Der optische Resonator wird dabei durch ein Kontrollfeld auf Resonanz für ω_s und ω_i gehalten. Die Wechselwirkung zwischen den Beteiligten drei Feldern führt zu einer Verstärkung der Felder bei ω_i und ω_s. Diese Verstärkung wiederum konkurriert mit den Verlusten, die zum einen durch Absorption im nichtlinearen Kristall und zum anderen durch Auskoppeln eines Teils der

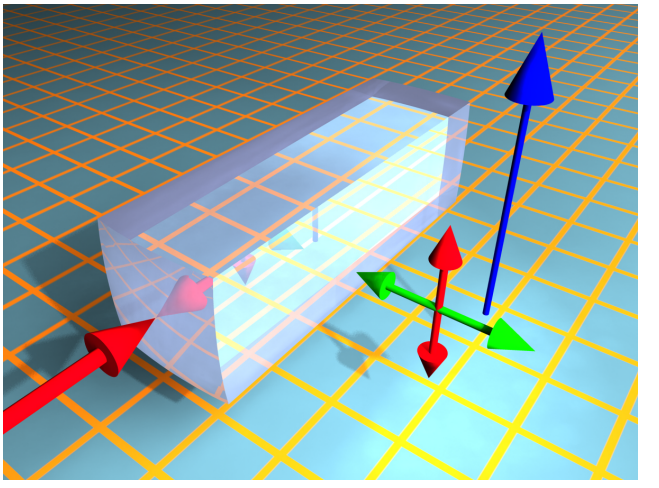

Abbildung 3.10 — Nichtlinearer Kristall und die beteiligten Richtungen. Der von links kommende rote Pfeil bezeichhnet die Achse der Pumpmode, der senkrechte Doppelpfeil die Polarisationsrichtung derselben. Der blaue Pfeil bezeichnet die außerordentliche Kristallachse. Der grüne Doppelpfeil bezeichnet die Polarisationsrichtung von Signal- und Idlerwelle.

Felder zustande kommen. Da der *gain* direkt von der Pumpleistung abhängt, die Verluste jedoch nicht, existiert eine Schwelle in der Pumpleistung, unterhalb derer die Dämpfung dominiert. In diesem Regime wird der OPA in dieser Arbeit zur Erzeugung von Squeezing betrieben.

3.5.5 Phasenanpassung

Will man die Wechselwirkung der unterschiedlichen Felder in einem nichtlinearen Kristall beschreiben, muß man die Ortsabhängigkeit der elektrischen Felder bedenken. Ein elektrisches Feld der Frequenz ω_p wird allgemein durch

$$E_p = \exp(i(\omega_p t - k_p x)) \tag{3.84}$$

beschrieben, wobei $k_p = n(\omega_p)\omega_p/c$ der Wellenvektor ist. Da der Brechungsindex des Kristalls von der Wellenlänge abhängt (Dispersion), kann offenbar nicht davon ausgegangen werden, dass sich Pumpfeld und Signal/Idler-Welle phasenstarr überlagern. Diese Bedingung muss hergestellt werden und wird als Phasenanpassung bezeichnet.

Tabelle 3.1 — Eine ausführliche Konvention zur Benennung der Phasenanpassung. Ein $\mathcal{E}$ bezeichnet die außerordentliche Kristallachse, ein $\mathcal{O}$ die ordentliche.

Pol. Pumpe	Pol. Signal	Pol. Idler	Bezeichnung
$\mathcal{E}$	$\mathcal{O}$	$\mathcal{O}$	Typ I
$\mathcal{E}$	$\mathcal{O}$	$\mathcal{E}$	Typ II (auch: Typ IIA)
$\mathcal{E}$	$\mathcal{E}$	$\mathcal{O}$	Typ III (auch: Typ IIB)
$\mathcal{E}$	$\mathcal{E}$	$\mathcal{E}$	Typ IV
$\mathcal{O}$	$\mathcal{O}$	$\mathcal{O}$	Typ V
$\mathcal{O}$	$\mathcal{O}$	$\mathcal{E}$	Typ VI (auch: Typ IIB oder IIIA)
$\mathcal{O}$	$\mathcal{E}$	$\mathcal{O}$	Typ VII (auch: Typ IIA oder IIIB)
$\mathcal{O}$	$\mathcal{E}$	$\mathcal{E}$	Typ VIII (auch: Typ I)

Typischerweise verfügt ein Kristall über drei optische Achsen, wobei eine Achse einen kleineren Brechungsindex ausweist als die anderen beiden. Diese Achse wird als außerordentliche Achse ($\mathcal{E}$) bezeichnet, die beiden anderen als ordentlich ($\mathcal{O}$). Es gibt prinzipiell drei Möglichkeiten, Phasenanpassung zu realisieren:

1 | Winkelanpassung. Phasenanpassung wird durch Drehen des Kristalls um einen kleinen Winkel erreicht. Nachteilig ist bei diesem Verfahren die Tatsache, dass die beteiligten Felder unterschiedlicher Frequenzen nicht mehr kollinear propagieren und damit die effektive Länge der Wechselwirkungszone (Überlapp der Moden) stark eingeschränkt wird.

2 | Quasi-Phasenanpassung. Diese erreicht man, indem man einen Kristall wählt, der periodisch gepolt ist. Hierbei wird der Kristall so gezogen, dass eine Kristallachse periodisch ihre Richtung umkehrt. Dann liegt in einem Kristallabschnitt für die Pumpwelle ein größerer Brechungsindex vor, im nächsten Kristallabschnitt für Signal/Idlerwelle. Wählt man das Polungsintervall hinreichend klein (typischerweise einige Mikrometer), erhält man eine näherungsweise Phasenanpassung.

3 | Temperaturanpassung. Diese Form der Phasenanpassung gelingt, wenn die Pumpwelle senkrecht zu Signal/Idler polarisiert ist. Man nutzt dann aus, dass die Doppelbrechung in einigen Kristallen (insbesondere in Lithiumniobat) stark von der Temperatur abhängt. Man versucht nun die Kristalltemperatur so einzustellen und zu regeln, dass die Dispersion durch die Doppelbrechung gerade ausgeglichen wird. Dieses Verfahren wird in der vorliegenden Arbeit umgesetzt.

Zur Klassifizierung der Phasenanpassung gibt es unterschiedliche Konventionen. Eine einfache und praktische Konvention spricht von einer Phasenanpassung vom „Typ I“, wenn Signal und Idlerwelle die gleiche Polarisation aufweisen und von „Typ II-Phasenanpassung“, wenn die beiden Felder senkrecht zueinander polarisiert sind. Daneben existiert eine komplexere Nomenklatur, die zu den Bezeichnungen aus ⇝Tabelle (3.1) führt.

KAPITEL 4

Theorie zur Destillation und Purifikation

4.1 Vorüberlegungen

4.1.1 Gaußsche Zustände und gaußsche Operationen

Es wurde in einem früheren Abschnitt argumentiert, dass die Durchführung von Quanteninformationsprotokollen mit kontinuierlichen Variablen verschiedene Vorteile gegenüber den traditionellen Ansätzen, die auf diskreten Variablen (*qbits*) basieren, bietet. Demzufolge sind in den letzten Jahren sehr erfolgreich eine ganze Reihe solcher Protokolle mit kontinuierlichen Variablen umgesetzt worden. Für einen guten und relativ aktuellen Überblick siehe [Bra05]. Bei all diesen Protokollen spielen *gaußsche Zustände* und *Gaußsche Operationen* eine zentrale Rolle. Als gaußsche Zustände bezeichnet man dabei solche Zustände, deren Wigner-Funktionen eine gaußsche Form aufweisen. Insbesondere hat die Wigner-Funktion eines *gequetschten* Zustandes gaußsche Form (jede Projektion entlang eines Quadraturwinkels entspricht einer gaußschen Verteilung von Messwerten in der orthogonalen Quadratur):

$$W(x,p) = \frac{1}{2\pi\sqrt{V_x V_p}} \exp\left(-\frac{\hat{x}^2}{2V_x} - \frac{\hat{p}^2}{2V_p}\right). \tag{4.1}$$

Betrachtet man solche gaußschen Zustände (die folglich eine gaußsche Verteilung der Messwerte in jeder Quadratur aufweisen), so können sehr viele

Tabelle 4.1 — Unitäre Operatoren, die wichtige gaußschen Operationen beschreiben. Häufig werden diese Operationen abhängig von $\hat{a}$ und $\hat{a}^\dagger$ geschrieben. In der hier angegebenen Darstellung mit den Quadraturoperatoren ist es einfacher, die Transformationen derselben abzuleiten.

Komponente	Operator
Strahlteiler	$\hat{U} = \exp(\frac{i\varphi}{4}(\hat{x}_1\hat{p}_2 - \hat{p}_1\hat{x}_2))$ mit $\varphi = 2\arccos(\sqrt{T})$
Phasenschieber	$\hat{U} = \exp(-\frac{i\theta}{4}(\hat{x}^2 + \hat{p}^2 - 2))$
Displacement	$\hat{U} = \exp(\frac{i}{2}(p_D\hat{x} - x_D\hat{p}))$
Squeezing	$\hat{U} = \exp(\frac{i\xi}{4}(\hat{x}\hat{p} + \hat{p}\hat{x}))$ mit $\xi = r\exp(i\theta)$

Quanteninformationsprotokolle ausschließlich durch die Verwendung linearer optischer Komponenten realisiert werden. Da die gaußsche Charakteristik der Zustände bei der Anwendung dieser Komponenten nicht verloren geht, bezeichnen wir solche Manipulationen als *Gaußsche Operationen*.

Erstaunlicherweise basieren fast alle Quanteninformationsprotokolle auf einer sehr begrenzten Anzahl von Operationen. Diese sind im einzelnen: lineare optische Komponenten (Strahlteiler), Quetschlichtquellen („Squeezer"), Homodyndetektoren und Einzelphotonendetektoren. Bis auf die zuletzt genannten Einzelphotonendetektoren (die in der vorliegenden Arbeit keine Rolle spielen und auch keine gaußsche Operation implementieren) stehen alle Komponenten in sehr guter Qualität zur Verfügung. Die hier betrachteten Komponenten Strahlteiler, Squeezer und Homodyndetektor implementieren also gaußsche Operationen (weitere lineare optische Komponenten, wie zum Beispiel Linsen, weisen triviale Transformationen auf und spielen für die prinzipielle Umsetzung eines Quanteninformationsprotokolls keine Rolle. Selbstverständlich sind komplexe optische Aufbauten ohne solche Komponenten nicht realisierbar).

Ist der Hamiltonoperator einer solchen Operation bekannt, kann man daraus einen unitären Entwicklungsoperator

$$\hat{U} = \exp(i\hbar\hat{H}t) \tag{4.2}$$

ableiten, der die Quadraturen eines Zustandes gemäß

$$\hat{x}_{\text{in}} \rightarrow \hat{x}_{\text{out}} = \hat{U}\hat{x}_{\text{in}}\hat{U}^\dagger \quad \text{und} \tag{4.3}$$

$$\hat{p}_{\text{in}} \rightarrow \hat{p}_{\text{out}} = \hat{U}\hat{p}_{\text{in}}\hat{U}^\dagger \tag{4.4}$$

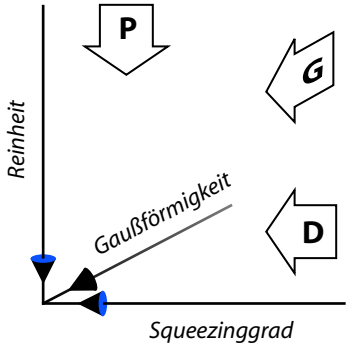

Abbildung 4.1 — Es sind drei Eigenschaften eines Zustandes, die bei den hier vorgestellten Protokollen eine Rolle spielen. Wir werden sehen, dass die Anwendung eines solchen Protokolls („Destillationsprotokoll“, „Purifikationsprotokoll“) den Squeezinggrad des Zustandes erhöht („Destillation“), die Reinheit des Zustandes vergrößert („Purifikation“) und die Messstatistik des Zustandes gaußförmiger werden läßt („Gaußifikation“).

transformiert. Eine Übersicht über die Operatoren von wichtigen gaußschen Operationen liefert ⇝Tabelle (4.1).

Es wurde bereits argumentiert, dass in jedem realistischen Szenario einer quantengestützten Kommunikation Störungen im Übertragungskanal die nichtklassischen Eigenschaften der übertragenen Zustände massiv beeinträchtigen (exponentielle Abhängigkeit von der physischen Länge des Kanals). Dies gilt nicht nur für die unmittelbare Übertragung von „Nachrichten“, die in nichtklassische Zustände hineinkodiert worden sind, sondern insbesondere auch für die Verteilung der Konstituenten eines verschränkten Paares zwischen den beiden Kommunikationspartnern. Wir hatten außerdem festgestellt, dass ein unmittelbares Analogon zu einem klassischen *repeater* (in Form einer – unter Umständen – mehrmaligen Nachvertärkung des Signals) nicht existiert. Der Ansatz mit diesem Problem umzugehen besteht darin, zu fragen, ob es möglich ist, aus einer großen Anzahl gemischter, schwach nichtklassischer Zustände eine kleinere Anzahl reiner, stark nichtklassischer Zustände zu generieren. Genau dieser Ansatz ist mit dem Begriff „Destillation“ (*distillation*) belegt worden [Ben96, Deu96]. Zwischenzeitlich ist die Nomenklatur in der Literatur ein wenig durcheinander geraten: Die Begriffe Destillation,

Purifikation und Konzentration werden dabei oft synonym gebraucht. Es wird in dieser Arbeit versucht, die folgende Konvention einzuhalten, die das „richtigste“ Benennungsschema darstellt: Wegen der großen Ähnlichkeit gequetschter und verschränkter Zustände und der Ähnlichkeit der Protokolle zur Bearbeitung der beiden, ist es nicht sinnvoll, in der Nomenklatur eine zusätzliche Unterscheidung zu realisieren. Wir sprechen in beiden Fällen von „Destillation“, wenn die nichtklassischen Eigenschaften verbessert werden. Von einer „Purifikation“ (*purification*) sprechen wir, wenn unter Anwendung eines Destillationsprotokolls die Reinheit der Zustände vergrößert wird. Es bietet sich an, als Begriff noch die „Gaußifikation“ einzuführen, die den Umstand bezeichnet, dass unter Anwendung eines Destillationsprotokolls die Ausgabezustände gaußförmiger werden.

Die Umsetzung eines solchen Destillations-Verfahrens ist im Regime von Zweizustandsystemen (qbits) vergleichsweise einfach zu realisieren [Eis02].

Man könnte also vermuten, dass ein solches Vorgehen auch bei Verwendung von kontinuierlichen Variablen zum Ziel führt. Ein umsetzbares, allgemeines Protokoll könnte dann etwa so aussehen, dass zwei verschränkte Paare A (bestehend aus den Konstituenten A_1 und A_2) und B (bestehend aus B_1 und B_2) vorbereitet und zwischen den Kommunikationspartnern aufgeteilt werden, so dass eine Partei („Sender“) über A_1 und B_1 verfügt und die andere Partei („Empfänger“) über A_2 und B_2. Jede Partei kann nun an ihren beiden Paaren beliebig lokale, unitäre Transformationen durchführen (Phasenverschiebungen, Strahlteiler, ...). Anschließend könnten Homodynmessungen an den Teilen A_2 und B_2 durchgeführt werden, wobei es den Kommunikationspartnern erlaubt ist, sich über einen klassischen Kommunikationskanal bezüglich der Messergebnisse zu verständigen. Anschließend könnten (etwa abhängig von den Messergebnissen) an dem verbliebenen verschränkten Paar weitere gaußsche Operationen durchgeführt werden (*Nachbearbeitung*).

Im Jahr 2002 erschienen drei Publikationen [Fiu02, Eis02, Gie02], die unabhängig voneinander zu dem sehr überraschenden Ergebnis kamen, dass keine Realisierung eines solchen Protokolls (nämlich der Destillation gaußscher Zustände mit lokalen gaußschen Operationen und klassicher Kommunikation (*local operations and classical communication,* LOCC)) eine Destillation der Verschränkung bewirkt. Tatsächlich erweist es sich als optimal, *gar nichts* zu unternehmen. Der präzise mathematische Beweis der Unmöglichkeit eines solchen Protokolls ist wenig instruktiv und wird daher nicht wiedergegeben. (Der Umstand der Unmöglichkeit einer Destillation gaußscher Zustände mit gaußschen Operationen (und klassischer Kommunikation) wird gelegentlich als „*no-go theorem*“ bezeichnet. Wir übernehmen diese Bezeichnung, weisen

aber darauf hin, dass dieses *Theorem* mathematisch erschöpfend bewiesen ist.)

Ein analoges *no-go theorem* ist in [Kra03] auch für gequetschte Zustände in der Form gezeigt worden, dass es nicht möglich ist, aus N Kopien eines gequetschten gaußschen Zustandes unter Verwendung von gaußschen Operationen eine Anzahl $M < N$ gequetschte Zustände mit höherem Quetschgrad als die ursprünglichen N Kopien zu *destillieren*. Damit ist die Unmöglichkeit eines Destillationsprotokolls für gequetschte Zustände gezeigt.

4.1.2 Nichtgaußsche Operationen

Um eine Destillation von Squeezing oder Verschränkung durchführen zu können, ist es also notwendig, den Bereich der gaußschen Operationen und/oder der gaußschen Zustände zu verlassen. Die experimentelle Umsetzung nichtgaußscher Operationen ist dabei mit besonderen Schwierigkeiten verbunden. Eine Möglichkeit besteht zum Beispiel darin, von einem gequetschten Strahl mittels eines Strahlteilers mit kleiner Reflektivität einen geringen Anteil abzuzweigen und mit einem Einzelphotondetektor zu detektieren. Man konditioniert dann auf das Vorhandensein eines einzelnen Photons im abgezweigten Ausgang (also auf den „Klick“ des Einzelphotonendetektors). Man kann in diesem Fall zeigen, dass im anderen Ausgang des Strahlteilers dann ein *Schrödinger cat state* vorliegt. Solche messungsindzierten nichtgaußschen Zustände können jedoch nur über Einzelphotonenmessungen erreicht werden. Durch die geringen Effizienzen der verfügbaren Detektoren (Größenordnung 10% bei 1064 nm) werden derartige Protokolle jedoch extrem ineffektiv und sind mit dem Anspruch einer Verwirklichung vor einem technologischen Hintergrund (der zwangsläufig hohe Bandbreiten fordert) nicht vereinbar.

Tatsächlich ist ein geeignetes Protokoll für die Destillation verschränkter Zustände, das auf diesem Prinzip beruht, von D. E. Browne und J. Eisert vorgeschlagen worden ([Bro03, Eis04]). Im ersten Schritt wird durch die konditionierte Subtraktion eines einzelnen Photons der zu bearbeitende Zustand *degaußifiziert*. In einem zweiten Schritt können die nun nichtgaußschen Zustände mittels linearer Operationen destilliert werden.

4.2 Phasenrauschen

Wir hatten bereits die Wignerfunktion eines gequetschten kohärenten Zustandes angegeben und festgestellt, dass diese einen gaußschen Zustand beschreibt. Eine Destillation des Quetschgrades eines solchen Zustandes ist

wegen des *no-go* Theorems bei Verwendung von lokalen gaußschen Operationen und klassischer Kommunikation (*local gaussian operations and classical communication,* LGOCC) ausgeschlossen. Um einen Ausweg zu finden, muss also das gaußsche Regime an mindesten einer Stelle verlassen werden. Bezüglich nichtgaußscher Operationen wurde argumentiert, dass deren experimentelle Umsetzung mit erheblichen Schwierigkeiten verbunden ist. Wir betrachten also erneut die gaußschen Zustände.

Dazu untersuchen wir die Wirkung des Phasenschiebe-Operators aus ⇝Tabelle (4.1). Die Quadraturoperatoren $\hat{x}$ und $\hat{p}$ eines kohärenten (und gegebenenfalls gequetschten) Zustandes transformieren unter Anwendung des Phasenschiebe-Operators wie

$$\hat{x} \quad \rightarrow \quad \hat{x}_\phi = \hat{U}\hat{x}\hat{U}^\dagger = \hat{x}\cos(\phi) + \hat{p}\sin(\phi) \quad \text{und} \tag{4.5}$$

$$\hat{p} \quad \rightarrow \quad \hat{p}_\phi = \hat{U}\hat{p}\hat{U}^\dagger = \hat{p}\cos(\phi) - \hat{x}\sin(\phi). \tag{4.6}$$

Die resultierende Wignerfunktion lautet

$$W(x,p) = \frac{1}{2\pi\sqrt{V_x V_p}} \exp\left(-\frac{\hat{x}_\phi^2}{2V_x} - \frac{\hat{p}_\phi^2}{2V_p}\right) \tag{4.7}$$

und ist für einige Werte von ϕ in ⇝Abbildung 4.2 exemplarisch gezeigt. Wir erinnern nun wieder an unser ursprüngliches Vorhaben, einen nichtklassischen Zustand in einem realistischen Kommunikationsszenario zwischen entfernten Kommunikationspartnern zu übertragen. Dies würde zum Beispiel per Transmission durch eine optische Faser (Länge in der Größenordnung $l \approx 10^3$ km) bewerkstelligt werden. Ein wichtiger Dekohärenzkanal bei Übertragung durch eine optische Faser ist das unvermeidlich auftretende Phasenrauschen. Wir modellieren diesen Vorgang, indem wir annehmen, dass bei der Übertragung statistisch *normalverteilte* Phasenverschiebungen auftreten, die in einem interessierenden Spektralbereich weiß über der Frequenz sein sollen. Ein solches Phasenrauschen wird durch die Standardabweichung σ vollständig charakterisiert und kann durch die gaußsche Wahrscheinlichkeitsverteilung

$$\Phi(\phi) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\phi^2}{2\sigma^2}\right) \tag{4.8}$$

beschrieben werden. Als Wahrscheinlichkeitsverteilung unterliegt $\Phi(\phi)$ der Normierung

$$\int \Phi(\phi) d\phi = 1. \tag{4.9}$$

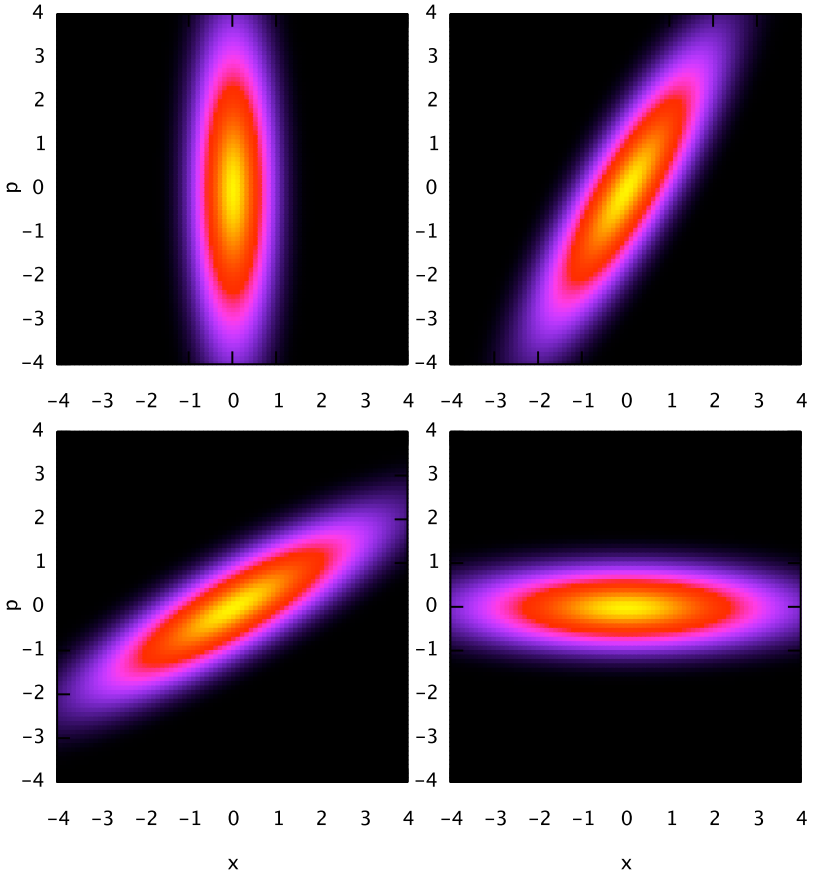

Abbildung 4.2 — Wignerfunktionen eines gequetschten gaußschen Zustandes nach Anwendung des Phasenschiebe-Operators für Phasenverschiebungen $\phi = 0°$, $\phi = 30°$, $\phi = 60°$ und $\phi = 90°$. Es ist augenfällig, wie die Anwendung des Phasenschiebeoperators eine Rotation der ellipsenförmigen Wignerkonturen im Phasenraum bewirkt.

Wird ein gaußscher und gequetschter kohärenter Zustand einem solchen Phasenrauschen unterworfen, geht seine Wignerfunktion über in [Fra06]

$$W_\Phi(x,p) = \frac{1}{2\pi\sqrt{V_x V_p}} \int \exp\left[-\frac{\hat{x}_\phi^2}{2V_x} - \frac{\hat{p}_\phi^2}{2V_p}\right] \Phi(\phi) d\phi. \tag{4.10}$$

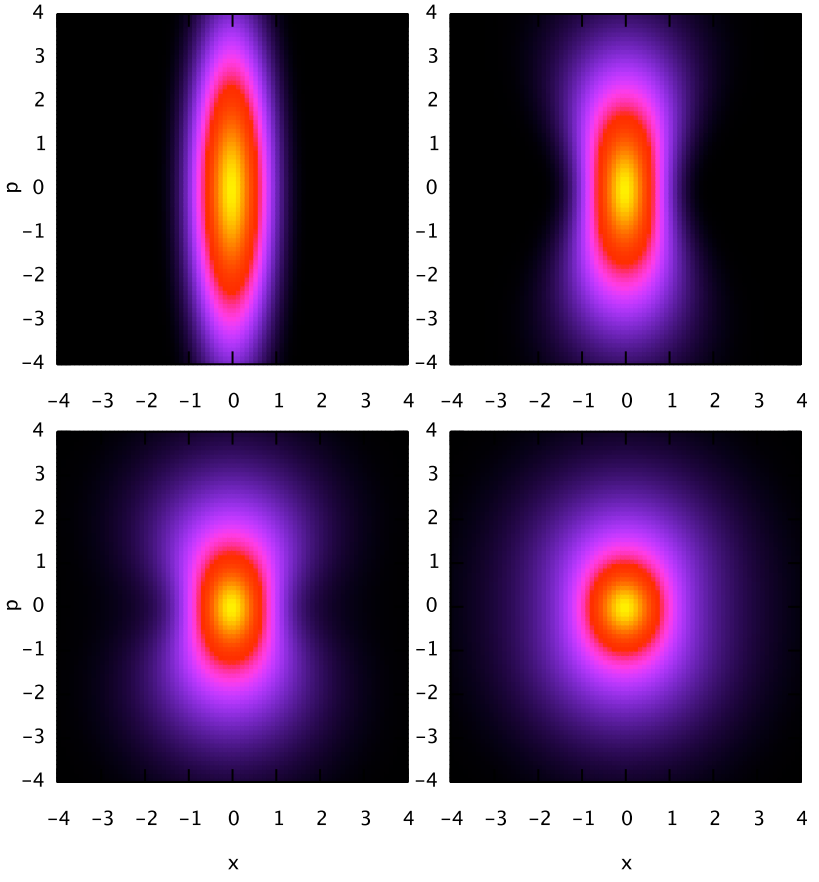

Abbildung 4.3 — Vier Wignerfunktionen von phasenverrauschten Zuständen. Von oben links ist zeilenweise die Stärke des Phasenrauschens erhöht worden. Oben links ist $\sigma = 0$, dann zeilenweise $\sigma = 0{,}3$, $\sigma = 0{,}6$ und $\sigma = 0{,}9$. Bereits durch Betrachten der gezeigten Wigner-Funktionen wird der Verdacht geweckt, dass phasenverrauschte Zustände keine gaußschen Zustände sind.

Solche phasenverrauschten Wignerfunktionen sind für verschiedene Werte von σ in ⇝Abbildung 4.3 gezeigt.

Betrachtet man die Wignerfunktionen aus ⇝Abbildung 4.3, so vermutet man bereits, dass diese einen nichtgaußschen Zustand beschreiben. Man kann sich davon überzeugen, dass dies tatsächlich der Fall ist, indem man Mar-

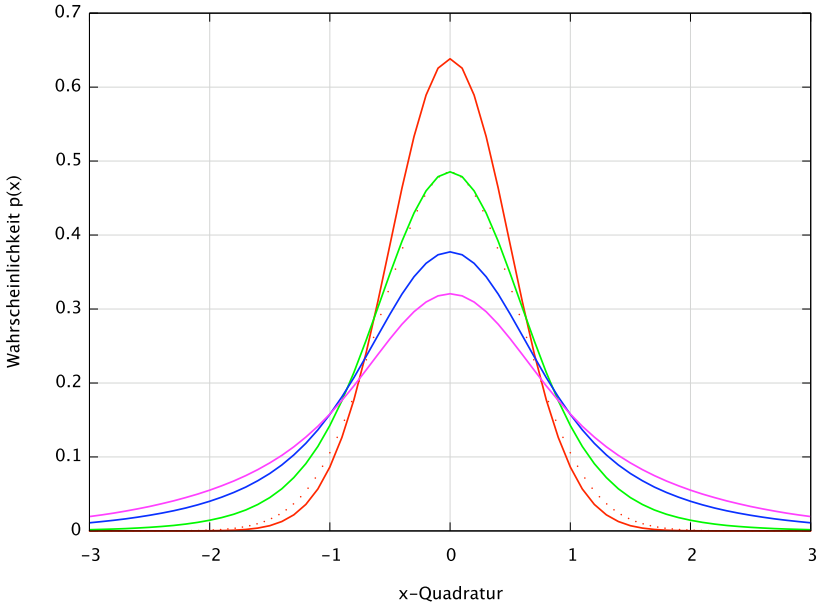

Abbildung 4.4 — Marginalwahrscheinlichkeitsverteilung von $\hat{x}$-Quadraturen von phasenverrauschten Zuständen für vier unterschiedliche Phasenrauschstärken mit $\sigma = 0$ (rot), $\sigma = 0{,}3$ (grün), $\sigma = 0{,}6$ (blau) und $\sigma = 0{,}9$ (violett), entsprechend den Wignerfunktionen aus ⇝Abbildung 4.3. Man erkennt, wie mit zunehmendem Phasenrauschen die Verteilung der Messwerte nicht mehr einer gaußschen Normalverteilung entspricht. Zum Vergleich ist als gepunktete Linie eine Gaußverteilung gezeigt, die in ihrer Amplitude der grünen Verteilung entspricht. Phasenrauschen transformiert also gaußsche Zustände auf nichtgaußsche Zustände.

ginalwahrscheinlichkeitsverteilungen aus den Wignerfunktionen generiert, zum Beispiel für die $\hat{x}$-Quadratur:

$$P_{\text{marg}}(x) = \int dp W(x,p). \tag{4.11}$$

Die sich ergebenden Wahrscheinlichkeitsverteilungen sind für vier verschieden große Standardabweichungen σ des Phasenrauschens in ⇝Abbildung 4.4 gezeigt. Mit steigender Phasenrauschstärke weicht die Verteilung der Messwerte der $\hat{x}$-Quadratur zunehmend von einer Normalverteilung ab. Es besteht kein Zweifel daran, dass dies auch für alle anderen Quadraturen in der gleichen Weise gilt. Diese Erkenntnis ebnet den Weg für das in dieser Arbeit vorgestellte Destillationsprotokoll, denn wir haben gerade gesehen,

dass ein über einen realistischen Kanal übertragener gequetschter Zustand also durch das unvermeidlich auftretende Phasenrauschen prinzipiell in einen nichtgaußschen Zustand überführt worden ist. Damit ist das *no-go* Theorem umgangen und eine Destillation des Quetschgrades ist nicht länger ausgeschlossen. Man beachte, dass die genaue Form des Phasenrauschens (die wir als gaußverteilt angenommen hatten) für das qualitative Funktionieren des im Folgenden beschriebenen Destillation- und Purifikationsprotokolls keine Rolle spielt.

4.3 Konstruktion eines Destillations-Protokolls

Unsere Strategie gibt vor, dass wir zwei Kopien eines gequetschten kohärenten Zustandes (die wir mit den Indizes A und B unterscheiden) betrachten. Die beiden Kopien werden über einen optischen Kanal übertragen und erleiden dabei unabhängig voneinander Phasenrauschen ϕ_A und ϕ_B. Durch dieses Phasenrauschen wird der Grad des Squeezings reduziert. Wir nehmen nun an, dass auf Seiten des Empfängers die beiden phasenverrauschten Zustände durch gaußsche Operationen manipuliert werden und untersuchen die Frage, ob es möglich ist, aus den beiden Kopien des Zustandes eine einzelne Kopie mit einem großeren Squeezinggrad zu erhalten.

Zu diesem Zweck werden die beiden Kopien des phasenverrauschten Zustandes phasenstarr auf einem 50:50-Strahlteiler überlagert. Wir unterscheiden im Folgenden die beiden Ausgangsfelder des Strahlteilers mit den Indizes 1 und 2, so dass etwa x_j die Amplitudenquadratur und p_j die Phasenquadratur im Ausgang $j = \{1, 2\}$ bezeichnet. In einem Ausgang des Strahlteilers (den wir als Purifikationsstrahlteiler bezeichnen) wird eine Homodyndetektion der Amplitudenquadratur x_1 durchgeführt. Findet man dabei für den erhaltenen Messwert, dass dieser *betragsmäßig kleiner* ist, als ein vorher fest gewählter Schwellenwert Q,

$$|x_1| < Q, \tag{4.12}$$

so wird der zum Zeitpunkt der Messung zeitgleich im anderen Ausgang des Purifikationsstrahlteilers vorliegende Zustand „akzeptiert“. Findet man dagegen, dass die ⇝Gleichung (4.12) nicht erfüllt ist, wird der Zustand „abgelehnt“.

Wir nehmen weiterhin an, dass vor der phasenrauschbehafteten Übertragung bei beiden Kopien die x-Quadratur gequetscht war, $V^x_{A|\text{ein}} < 1$,

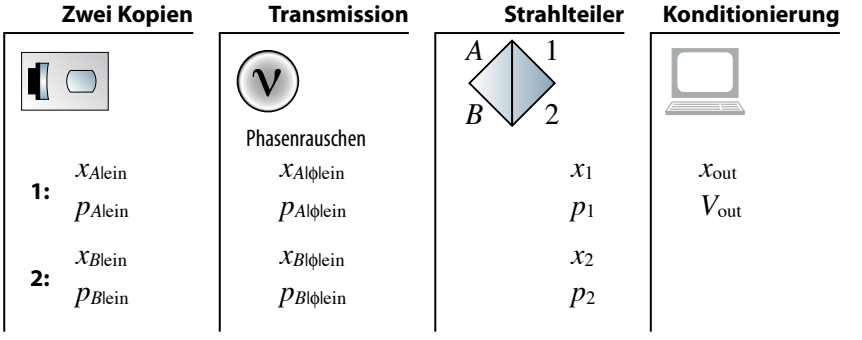

Abbildung 4.5 — Benennungsschema der unterschiedlichen Quadraturoperatoren und der korrespondierenden Varianzen.

$V^x_{B|\text{ein}} < 1$, und dass in jeder Kopie keine Korrelation zwischen x- und p-Quadratur besteht. Da es sich um Kopien desselben Zustandes handelt, gilt außerdem:

$$V^x_{A|\text{ein}} = V^x_{B|\text{ein}} =: V_x, \tag{4.13}$$

$$V^p_{A|\text{ein}} = V^p_{B|\text{ein}} =: V_p. \tag{4.14}$$

Wir betrachten für den Moment den Fall, dass die Phasenverschiebungen Φ_A und Φ_B auf Werte ϕ_A und ϕ_B festgehalten sind. Die Varianzen der beiden phasenverschobenen Moden, die sich am Purifikationsstrahlteiler überlagern, lauten dann:

$$V_{x|\phi|A} = V_x \cos^2(\phi_A) + V_p \sin^2(\phi_A), \tag{4.15}$$

$$V_{x|\phi|B} = V_x \cos^2(\phi_B) + V_p \sin^2(\phi_B), \tag{4.16}$$

$$V_{p|\phi|A} = V_p \cos^2(\phi_A) + V_x \sin^2(\phi_A), \tag{4.17}$$

$$V_{p|\phi|B} = V_p \cos^2(\phi_B) + V_x \sin^2(\phi_B). \tag{4.18}$$

Die x-Quadraturen in den beiden Ausgängen des Purifikationsstrahlteilers lauten nach der Überlagerung (siehe hierzu die Strahlteilergleichungen in ⇝Anhang (B)).

$$x_1 = \frac{1}{\sqrt{2}}(x_{A|\phi|\text{ein}} + x_{B|\phi|\text{ein}}), \tag{4.19}$$

$$x_2 = \frac{1}{\sqrt{2}}(x_{B|\phi|\text{ein}} - x_{A|\phi|\text{ein}}). \tag{4.20}$$

Die Verbundwahrscheinlichkeitsverteilung zwischen der vermessenen Quadratur x_1 in einem Ausgang des Purifikationsstrahlteilers und der Amplitudenquadratur x_2 im zweiten Ausgang, also die Wahrscheinlichkeit, das Wertepaar (x_1, x_2) zu messen, lautet dann:

$$P(x_1, x_2) = \frac{1}{2\pi\sqrt{V_{x1}V_{x_2}}} \exp\left[-\frac{A(x_1^2 + x_2^2) - 2Bx_1x_2}{2(A^2 - B^2)}\right]. \tag{4.21}$$

Dabei haben wir zur Abkürzung gesetzt

$$A = \frac{1}{2}(V_{x1} + V_{x2}) \quad \text{und} \quad B = \frac{1}{2}(V_{x2} - V_{x1}). \tag{4.22}$$

Konditioniert man diese Wahrscheinlichkeitsverteilung nun auf die uns interessierenden Fälle, dass der Zustand im zweiten Ausgang des Purifikationsstrahlteilers „akzeptiert" wird, also auf $|x_1| < Q$, so kann man die konditionierte Wahrscheinlichkeitsverteilung angeben:

$$P_{\text{cond}}(x_2) = \int_{-Q}^{Q} P(x_1, x_2)dx_1. \tag{4.23}$$

Die Verteilung der resultierenden Quadratur x_2 erhält man, indem man über die auftretenden Phasenverschiebungen mittelt. Dies führt auf

$$P_{\text{out}}(x_2) = \frac{1}{\mathcal{P}} \int_{\phi_A} \int_{\phi_B} P_{\text{cond}}(x_2)\Phi(\phi_A)\Phi(\phi_B)d\phi_A d\phi_B \tag{4.24}$$

mit einem Normierungsfaktor

$$\mathcal{P} = \int_{\phi_A} \int_{\phi_B} \text{erf}\left(\frac{Q}{\sqrt{2A}}\right) \Phi(\phi_A)\Phi(\phi_B)d\phi_A d\phi_B. \tag{4.25}$$

Geht man nun davon aus, dass die Phasenverschiebungen einen Mittelwert von Null haben, also symmetrisch sind ($\Phi(\phi) = -\Phi(\phi)$), so ist auch der Mittelwert der Ausgangsquadraturwerte gleich Null $\langle x_2 \rangle = 0$. Damit ist die Ausgangsvarianz gleich $\langle x_2^2 \rangle$. Man findet

$$V_{\text{out}} = \frac{1}{\mathcal{P}} \int_{\phi_A} \int_{\phi_B} \left[A\text{erf}\left(\frac{Q}{\sqrt{2A}}\right) - \sqrt{\frac{2}{\pi}}\frac{B^2 Q}{A^{3/2}} e^{-Q^2/2A}\right] \Phi(\phi_A)\Phi(\phi_B)d\phi_A d\phi_B. \tag{4.26}$$

Dies vergleicht man mit der Varianz eines einzelnen phasenverrauschten Zustandes

$$V_{\text{in}} = \int_{\phi} (V_x \cos^2(\phi) + V_p \sin^2(\phi))d\phi. \tag{4.27}$$

Eine erfolgreiche Destillation findet statt, falls $V_{\text{out}} < V_{\text{in}}$, denn in diesem Fall ist die Varianz des konditionierten Zustandes kleiner (sein Quetschgrad also größer), als die jeder einzelnen phasenverrauschten Kopie. Man beachte, dass stets $V_{\text{out}} > V_x$, es ist also in keinem Fall möglich, einen Quetschgrad zu erreichen, der größer ist, als der Quetschgrad der ursprünglichen Zustände vor Anwendung des Phasenrauschens.

4.4 Veranschaulichung des Destillationsprotokolls

Das Destillationsprotokoll des vorhergehenden Abschnittes kann anschaulich vergleichsweise leicht verstanden werden. Dazu betrachten wir die zwei Kopien eines gequetschten Zustandes, die am Purifikationsstrahlteiler überlagert werden, nachdem sie zufälligem Phasenrauschen unterworfen wurden. Wir hatten gesehen, dass solche Phasenverschiebungen eine Rotation der ellipsenförmigen Wignerfunktionen im Phasenraum verursachen. Die beiden phasenverschobenen Zustände haben Amplitudenquadraturen $x_{A|\phi|\text{ein}}$ und $x_{B|\phi|\text{ein}}$. Nach der Überlagerung am Strahlteiler liegen in den beiden Ausgängen desselben die beiden Zustände mit Amplitudenquadraturen

$$x_1 = \frac{1}{\sqrt{2}}(x_{A|\phi|\text{ein}} + x_{B|\phi|\text{ein}}) \tag{4.28}$$

und

$$x_2 = \frac{1}{\sqrt{2}}(x_{B|\phi|\text{ein}} - x_{A|\phi|\text{ein}}) \tag{4.29}$$

vor. Mit einem Homodyndetektor vermessen wir x_1 und konditionieren auf $|x_1| < Q$. Falls diese Bedingung erfüllt ist, wird der Zustand x_2 im anderen Ausgang des Purifikationsstrahlteilers „akzeptiert“, andernfalls „abgelehnt“.

Die Funktion des Protokolls kann man nun veranschaulichen, wenn man eine „Momentaufnahme“ betrachtet, in der die beiden Kopien eines gequetschten Zustandes jeweils eine *feste* Phasenverschiebung ϕ_A und ϕ_B erfahren. Wir betrachten nun zunächst den Spezialfall, dass die Phasendifferenz $\pi/2$ betrage, etwa $\phi_A = 0$ und $\phi_B = \pi/2$. Werden diese beiden Zustände an einem Strahlteiler überlagert, so erhält man in den beiden Ausgängen des Strahlteilers zwei Zustände, deren Wignerfunktionen einem thermisch angeregten Zustand entsprechen, also keine Zustände minimaler Unschärfe sind. Die bei einer Quadraturmessung zu erhaltenden Messwerte weisen jedoch eine nichtklassische Korrelation (Verschränkung) auf. Genau diese Korrelation wird

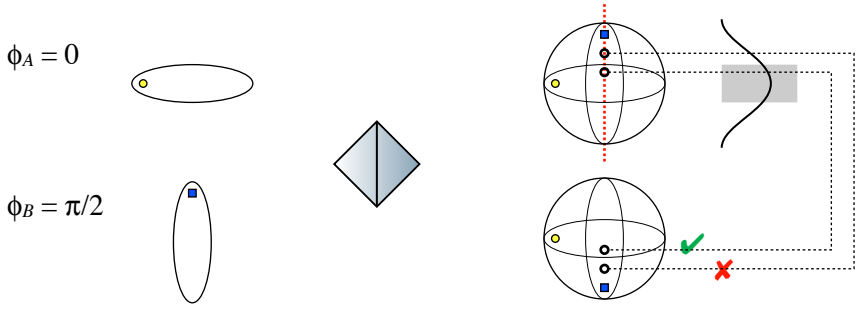

Abbildung 4.6 — Ein anschauliches Erklärungsmodell für das Funktionieren des Destillationsprotokolls, das auf einer Messung von x_1 basiert und auf die Bedingung $|x_1| < Q$ konditioniert. Es wird der Spezialfall betrachtet, in dem die Phasenverschiebungen $\phi_A = 0$ und $\phi_B = \pi/2$ betragen. Die beiden Zustände in den Ausgängen des Purifikationsstrahlteilers weisen eine nichtklassische Korrelation (Verschränkung) auf. Erhält man bei Vermessung der ursprünglich gequetschten Quadratur in einem Ausgang des Strahlteilers einen Wert Nahe bei Null, so erhält man mit großer Wahrscheinlichkeit auch am zweiten Zustand einen Wert Nahe bei Null. Setzt man zur Selektion ein Kriterium wie $|x_1| < 0$ an, selektiert man also Messwerte, die einer schmalen Verteilung folgen.

beim destillieren ausgenutzt: Liefert etwa eine Messung der ursprünglich gequetschten Quadratur im einem Ausgang des Purifikationsstrahlteilers einen Wert *nahe bei Null*, der dann also das Konditionierungskriterium $|x_1| < Q$ besteht, so erhält man auch bei Messung der ursprünglich gequetschten Quadratur des Zustandes im anderen Ausgang des Purifikationsstrahlteilers einen Wert *nahe bei Null*. Bei diesem Vorgehen werden also im zweiten Ausgang des Strahlteilers gerade die Messwerte selektiert, die eine schmale Verteilung bilden (⇝Abbildung 4.6).

In gleicher Weise argumentiert man in den Fällen, in denen der Phasenunterschied zwischen den beiden Kopien nach wie vor $\pi/2$ beträgt, aber $\phi_A, \phi_B \neq 0$, denn auch dann sorgt die Verschränkung der Zustände in den beiden Ausgängen des Purifikationsstrahlteilers für eine nichtklassische Korrelation der Messwerte.

Beträgt die relative Phasenverschiebung der beiden Zustände weniger als $\pi/2$, so nimmt die Stärke der Verschränkung zwischen den beiden Zuständen in den Ausgängen des Purifikationsstrahlteilers ab und das Destillationspro-

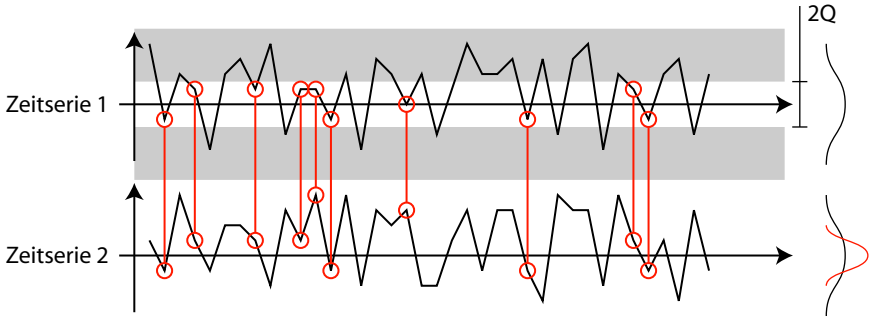

Abbildung 4.7 — Man betrachtet zwei Zeitserien von Messwerten der Amplitudenquadraturen von den beiden Zuständen in den Ausgängen des Purifikationsstrahlteilers. Ein Messwert im zweiten Ausgang wird akzeptiert, wenn der korrespondierende Messwert im ersten Ausgang betragsmäßig kleiner ist als ein Schwellenwert Q. Die derart ausgewählten Werte aus Zeitserie 2 besitzen eine kleinere Varianz als die Gesamtheit der Messwerte.

tokoll wird weniger effizient. Dem entgegen wirkt der Effekt rein klassischer Korrelation: Betrachtet man den Grenzfall verschwindender relativer Phasenverschiebung, sind die Quetschellipsen also nahezu parallel ausgerichtet, so werden die Messwerte im einen Ausgang des Strahlteilers aus der schmalen Verteilung der gequetschten Quadratur gezogen. Dies entspricht einer hohen Wahrscheinlichkeit für kleine Messwerte, das Konditionierungskriterium wird also von vielen Messwerten erfüllt. In diesem Fall werden aber auch die Messwerte im zweiten Ausgang des Strahlteilers aus der schmalen Verteilung der gequetschten Quadratur gezogen. Das Protokoll funktioniert also auch in diesem Fall, jedoch ohne die Quanteneigenschaften der Zustände auszunutzen.

Wir betrachten nun den Fall, dass die relative Phasenverschiebung der beiden Kopien nahe bei Null ist, also nur wenig Verschränkung vorliegt, allerdings $\phi_A \approx \phi_B$ in der Nähe von $\pi/2$ ist. In diesem Fall realisieren sich im zweiten Ausgang des Strahlteilers Messwerte, die aus der breiten Verteilung der antigequetschten Quadratur gezogen werden. Genau in diesem ungünstigen Fall vermisst aber auch der Homodyndetektor im ersten Ausgang des Purifikationsstrahlteilers die antigequetschte Quadratur, da wir angenommen hatten, dass die relative Phasenverschiebung klein sein soll. Es ist damit also unwahrscheinlich (allerdings keinesfalls ausgeschlossen!), dass die Konditionierungsbedingung erfüllt wird und der Zustand x_2 akzeptiert wird.

Genau die Tatsache, dass auch diese „schlechten“ Zustände mit endlicher Wahrscheinlichkeit akzeptiert werden, bewirkt, dass durch einmalige Destillation im Fall endlichen Squeezings das Ursprungssqueezing nicht vollständig zurück erhalten werden kann.

4.5 Wirkungsweise des Destillationsprotokolls

Wir wollen nun die Wirkungsweise des oben konstruierten Destillationsprotokolls auf zwei Kopien eines gequetschten Zustandes demonstrieren. Dazu können die hergeleiteten Gleichungen analytisch oder numerisch (Lösen der Integrale) ausgewertet werden. Wir verwenden im Rahmen dieser Arbeit allerdings einen anderen Ansatz, der auf einer rein numerischen *Simulation* der Vorgänge bei der Destillation basiert. Die Funktionsweise der Simulation wird in Kapitel 6 detailliert erläutert – wir beschränken uns an dieser Stelle zunächst auf eine einfache Demonstration. Wie wir in einem späteren Abschnitt sehen werden, weist das eingeführte Destillationsprotokoll eine weitaus größere Anzahl an Möglichkeiten auf, als die naive Einführung zunächst vermuten lassen würde. Tatsächlich wurde diese Reichhaltigkeit des Protokolls durch experimentelle Befunde entdeckt, die dann eine Weiterentwicklung und eine detailliertere Analyse der Theorie nach sich zogen, die die zusätzlichen Möglichkeiten in vollem Umfang bestätigt hat. Diese Entwicklung wird im Kapitel 7 detailliert nachvollzogen.

Hier betrachten wir zunächst nur den Fall zweier Kopien, die über jeweils 6 dB nichtklassischer Rauschunterdrückung verfügen. Numerisch werden diese Zustände mit einem zufälligen Phasenrauschen (gaußscher Verteilung) versehen und gemäß dem oben eingeführten Protokoll ausgewertet. Die ⇝Abbildung 4.8 zeigt eine solche Auswertung für die beiden Kopien eines gequetschten Zustandes für drei unterschiedliche Standardabweichungen σ des Phasenrauschens. Dargestellt wird jeweils die Varianz des konditionierten Ausgabezustandes über unterschiedlichen Schwellenwerten Q. Man erkennt zunächst, wie der Quetschgrad von ursprünglich 6 dB mit zunehmender Stärke des Phasenrauschens immer weiter reduziert wird. Für einen gewissen Wert des Phasenrauschens liegt die Varianz der ursprünglich gequetschten Quadratur oberhalb des Vakuumrauschens, die Zustände sind also nicht länger gequetscht. Führt man nun das Destillationsprotokoll wie beschrieben durch und wählt den Schwellenwert zunehmend kleiner, wird dadurch monoton die Varianz wieder verkleinert. Betrachtet man in ⇝Ab-

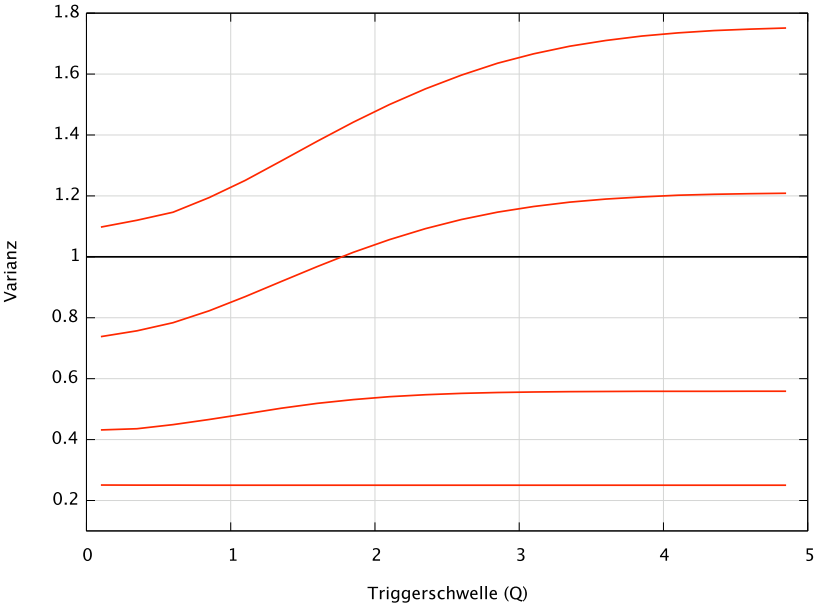

Abbildung 4.8 — Wirkungsweise des beschriebenen Destillationsprotokolls bei Verwendung zweier Zustände mit jeweils $V_x = 0{,}25$ und $V_p = 4$, entsprechend einer nichtklassischen Rauschunterdrückung von -6 dB. Die Nichtklassizität der Zustände wird durch Phasenrauschen mit vier unterschiedlichen Standardabweichungen σ beeinträchtigt.Von unten nach oben: $\sigma = 0{,}0$, $\sigma = 0{,}3$, $\sigma = 0{,}6$ und $\sigma = 0{,}9$ (vergleiche die Wignerfunktionen aus ⇝Abbildung 4.3). Man erkennt, wie durch eine kleiner werdende Wahl des Schwellenwertes Q die nichtklassische Rauschunterdrückung des destillierten Zustandes wieder zunimmt. Mit steigender Phasenrauschstärke wird das Protokoll zunehmend effektiver. Bemerkenswert ist der Fall $\sigma = 0{,}6$. Vor Anwendung des Destillationsprotokolles war die nichtklassische Eigenschaft des Zustandes vollständig verloren. Die Destillation bringt nun die Varianz des Ausgabezustandes unter das Vakuumrauschen zurück, womit der Ausgabezustand wieder gequetscht ist.Man erkennt auch, dass im Fall verschwindenden Phasenrauschens die Destillation keinen Effekt hat (und auch nicht haben kann, da das Destillationsprotokoll die Varianz nicht unter die Eingangsvarianz bringen kann).

bildung 4.8 etwa die Kurve, die zu $\sigma = 0{,}6$ gehört, erkennt man, dass für die Wahl $Q \approx 1{,}7$ von der Varianz des Ausgabezustandes das Vakuumrauschen wieder durchbrochen wird. Für noch kleinere Werte von Q liegt die Varianz unter 1 – der Ausgabezustand ist unter Anwendung des Destillationsprotokolls wieder gequetscht worden! Für starkes Phasenrauschen kann durch

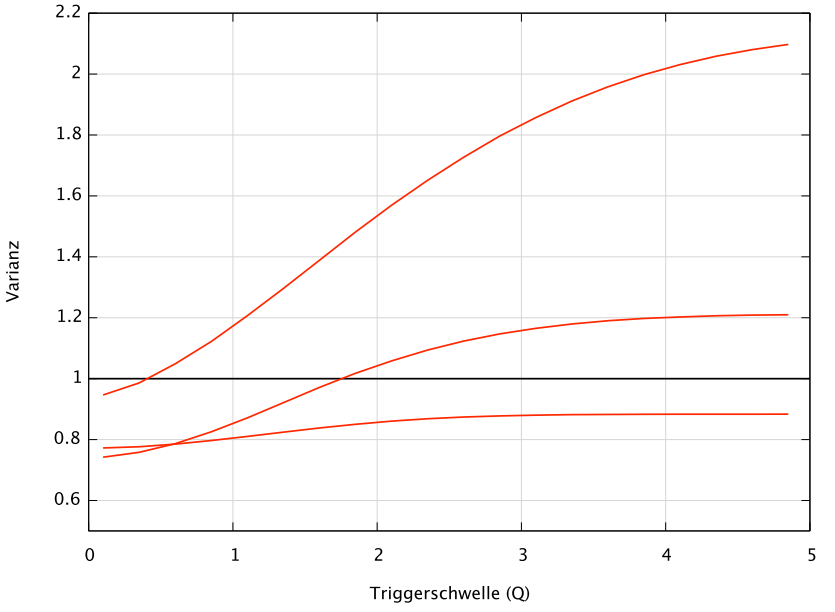

Abbildung 4.9 — Wirkung des Destillationsprotokolls auf Zustände mit unterschiedlichem Quetschgrad. Drei Zustände mit 3 dB, 6 dB und 9 dB Squeezing sind jeweils Phasenrauschen mit der gleichen Standardabweichung $\sigma = 0{,}6$ unterworfen worden. Man erkennt, wie die Eingangszustände mit wachsendem Squeezinggrad zunehmend empfindlicher gegen Phasenrauschen werden. Auf der anderen Seite ist die Destillation mit zunehmender Rauschunterdrückung der Eingabezustände zunehmend effektiver (höherer Destillationsgrad).

einmalige Anwendung des Protokolls keine Reduktion der Varianz unter das Vakuumrauschen mehr erreicht werden.

In der ⇝Abbildung 4.9 ist eine Auswertung für festes Phasenrauschen $\sigma = 0{,}6$ aber unterschiedlichem Quetschgrad der beiden Kopien gezeigt. Man erkennt, wie Zustände höheren Quetschgrades zunehmend empfindlicher gegen *dasselbe* Phasenrauschen werden (Ursache ist das bei diesen Zuständen ebenfalls größere Antisqueezing in der antigequetschten Quadratur). Man sieht außerdem, dass das maximal zurückgewinnbare Squeezing (für kleine Schwellenwerte Q) *keine* monotone Funktion des ursprünglichen Squeezings ist.

KAPITEL 5

Experimentelle Umsetzung

5.1 Überblick

Alle in dieser Arbeit dargestellten Ergebnisse konnten an einem einzigen optischen Aufbau gewonnen werden. Die verschiedenen Experimente erfordern jeweils lediglich kleinere Änderungen der Kontrollelektronik. Der Gesamtaufbau kann dabei in drei Funktionsgruppen unterteilt werden:

1 | Erzeugung = *Generation stage*. Dieser Teil des optischen Aufbaus diente der Bereitstellung von zwei Kopien eines gequetschten Zustandes. Die Erzeugung dieser Zustände gelang mit zwei OPAs, die von einer gemeinsamen Laserquelle (Nd:YAG, 1064 nm) gepumpt wurden.

2 | Übertragung = *Transmission stage*. Die zweite Sektion des Experiments emulierte die Übertragung der beiden gequetschten Zustände durch einen optischen Kanal. Dabei wurden die beiden Zustände mit zufälligem Phasenrauschen versehen.

3 | Purifikation/Detektion = *Purification stage/Detection stage*. Im letzten Abschnitt wurde der optische Anteil der Purifikation vollzogen. Außerdem erfolgte die Detektion und Erfassung der Zustände mittels Homodyndetektion.

Im Grunde könnte an dieser Stelle ein vierter Abschnitt eingeführt werden, der die Nachbearbeitung der Daten beschreibt. Dieser ist zwar ein wesentlicher Bestandteil der dargestellten Purifikationsprotokolle, kann jedoch zeitlich

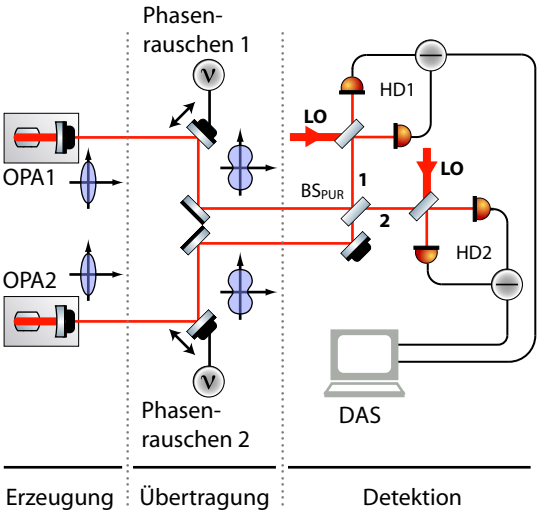

Abbildung 5.1 — Schematische Übersicht über den experimentellen Aufbau. Der Gesamtaufbau kann in die drei Funktionsgruppen „Erzeugung“, „Übertragung“ und „Detektion“ unterteilt werden. Zwei OPAs erzeugen zwei Kopien eines gequetschten Zustandes, die unabhängig voneinander mit weißem Phasenrauschen gaußscher Gewichtung im Frequenzband 1–5 kHz versehen werden. Die beiden Strahlen werden dann auf einem Strahlteiler (BS$_{PUR}$) phasenstarr überlagert. Ein Datenaufnahmesystem registriert simultan Zeitserien von Messwerten, die die beiden Homodyndetektoren HD1 und HD2 in den Ausgängen von BS$_{PUR}$ liefern.

und räumlich getrennt vom experimentellen Aufbau durchgeführt werden und wird daher von diesem gelöst betrachtet.

Bedenkt man ein „realistisches“ Szenario aus dem Bereich der Quanteninformation, bei dem es darum geht, eine quantengestützte Kommunikation zwischen zwei räumlich getrennten Parteien zu ermöglichen, so würde man die Erzeugung und Vorbereitung der Zustände auf Seiten eines „Senders“ ansiedeln. Die Übertragung repräsentiert dann einen optischen Kanal zwischen „Sender“ und „Empfänger“ (zum Beispiel eine optische Faser erheblicher Länge). Die Purifikation und Detektion (inklusive der Nachbearbeitung der Daten) erfolgt allein auf Seiten des „Empfängers“. Die drei Abschnitte „Erzeugung“, „Übertragung“ und „Detektion“ werden in den folgenden drei Abschnitten detailliert besprochen.

5.2 Erzeugung

5.2.1 Laser

Als Laser wurde ein kommerziell erhältliches Lasersystem vom Typ DIABOLO der Firma INNOLIGHT verwendet. Das laseraktive Medium dieses Festkörperlasers (Funktionsprinzip: NPRO) besteht aus mit Nd^{3+}-Ionen dotiertem $Y_3Al_6O_{12}$ (Yttrium-Aluminium-Granat = YAG). Die Ausgangsleistung dieser Lasers betrug circa 2 W bei einer Wellenlänge von 1064 nm. Etwa 1,7 W dieses Laserfeldes wurden noch im Lasersystem frequenzverdoppelt. Dieses zusätzliche Feld bei 532 nm verfügte dann über eine Leistung von etwa 800 mW und diente als Pumpfeld für die OPAs. Die verbleibenden 300 mW bei 1064 nm dienten einerseits als Kontrollfelder für die OPAs (gelegentlich als *„seed"* bezeichnet), andererseits als Lokaloszillatoren, die in der Detektion benötigt wurden.

5.2.2 Optisch parametrische Verstärker (OPAs)

Als Quelle gequetschter Zustände wurden zwei identisch konstruierte OPAs verwendet. Ein solcher OPA war um einen nichtlinearen MgO:$LiNbO_3$-Kristall herum konstruiert. Der Dotierungsgrad der verwendeten Kristalle betrug dabei 7 mol %. Beide Endflächen des Kristalles waren sphärisch konvex gekrümmt mit einem Krümmungsradius von 8 mm (Flächengenauigkeit $\lambda/10$). Die Abmessungen der Kristalle betrugen lediglich $6{,}5 \times 2{,}5 \times 2{,}0\ \mathrm{mm}^3$. Um die nichtlineare Wechselwirkung zwischen den beiden beteiligten Feldern zu vergrößern, ist es wesentlich, den Kristall im Innern eines optischen Resonators unterzubringen. Zu diesem Zweck war eine Endfläche des Kristalls hochreflektiv für 1064 nm beschichtet ($r^2 > 0.999$). Prinzipiell könnte die andere Endfläche des Kristalls ebenfalls eine solche Beschichtung tragen und damit den Resonator abschließen. Tatsächlich sind solche (sogenannten *monolithischen*) Konstruktionen erfolgreich zur Erzeugung von – insbesondere hohen – Squeezinggraden eingesetzt worden. In diesem Fall müßte jedoch die Laserfrequenz geregelt werden um mit diesem Resonator resonant zu sein. Dann ist es aber nicht mehr ohne weiteres möglich, einen baugleichen zweiten OPA zu betreiben. Wir verwendeten daher ein *hemilithisches* (halb-monolithisches) Design, bei dem das zweite Resonatorende durch einen externen Auskoppelspiegel gestellt wurde. Dieser Auskoppelspiegel hatte einen Durchmesser von 12,7 mm und eine Reflektivität (bei 1064 nm) von $r^2 = 0{,}947$. Der Spie-

gel war meniskusförmig und hatte einen Krümmungsradius von 25 mm auf der Resonatorseite und einen Krümmungsradius von 20 mm auf der dem Resonator abgewandten Außenseite. Diese Konstruktion ist an die stark divergente Resonatormode angepasst und hat zum Ziel, die Linsenwirkung einer planen Grenzfläche auf eine stark divergente Mode zu reduzieren. Die Wahl der Reflektivität des Auskoppelspiegels beruht wesentlich auf Erfahrungen und stellt einen Kompromiss dar: Einerseits will man eine hohe Umlaufzeit im Resonator erzielen (Vergrößerung der nichtlinearen Wechselwirkungsstrecke), andererseits will man die beim Umlauf des Feldes erlittenen Verluste (Absorption) gering halten. Die Resonatorlänge wurde geregelt, indem man durch die hochreflektierende Schicht des Kristalls ein Kontrollfeld (typische Leistung: 15 mW) einstrahlt. Trägt dieses Feld eine Phasenmodulation, kann nach Detektion des reflektierten Feldes eine Regelung der Resonatorlänge nach dem Pound-Drever-Hall-Verfahren angewendet werden [Bla00]. Das erzeugte Stellsignal für die Resonatorlänge wurde dabei auf einen piezoelektrischen Kristall gegeben, der den Auskoppelspiegel trieb und damit die Resonatorlänge steuerte.

Das für den nichtlinearen Prozess notwendige Pumpfeld bei 532 nm (Kapitel 3) wurde durch den Auskoppelspiegel hindurch in den längengeregelten Resonator eingestrahlt. Die hochreflektiv abgeschlossene Kristallseite war auch für 532 nm mit einer hochreflektierenden Beschichtung versehen, wohingegen der Auskoppelspiegel für 532 nm lediglich eine kleine Reflektivität von $r^2 = 0{,}15 \pm 0{,}02$ aufwies. Die verbleibende Kristallfläche im Innern des Resonators war mit einer Antireflexschicht versehen ($r^2 < 0{,}05\%$ für 1064 nm, $r^2 < 0{,}2\%$ für 532 nm).

Da die Phasenlage zwischen rotem und grünem Feld im Resonator ebenfalls geregelt werden muss, wurde das grüne Feld über einen piezogetriebenen Planspiegel in den Resonator hinein reflektiert. Die Extraktion eines Fehlersignals erfolgte ebenfalls auf dem aus dem Resonator stammenden Feld, das bereits für die Längenregelung verwendet wird. Nach einem von B. Hage (nicht veröffentlicht) entwickelten Verfahren wurde dabei mit einer um 90 Grad verschobenen Phase (bezüglich der Demodulation für das Längenfehlersignal) demoduliert. Die Vorteile dieses Vorgehens liegen auf der Hand: Es wird lediglich ein einziger Photodetektor benötigt und es ist nicht nötig, auf dem gequetschten Feld, das den Resonator durch den Auskoppelspiegel verläßt, zu detektieren. Weiter ist es nicht nötig, dass das grüne Feld eine eigene Modulation trägt.

Man kann die Güte eines Resonators durch die sog. Finesse $\mathcal{F}$ beschreiben.

Tabelle 5.1 — Übersicht über die Reflektivitäten, die beim OPA-Design eine Rolle spielen. HR: Hochreflektierende Beschichtung, AR: Antireflex-Beschichtung.

Auskoppelspiegel			
AR:	1064 nm	$r^2 < 0{,}15\%$	$i = 0° - 20°$
	532 nm	$r^2 < 0{,}2\%$	$i = 0° - 20°$
HR:	1064 nm	$r^2 = 94{,}7\% \pm 0{,}4\%$	$i = 0°$
	532 nm	$r^2 = 15\% \pm 2\%$	$i = 0°$
Kristall			
AR:	532 nm	$r^2 < 0{,}2\%$	
	1064 nm	$r^2 < 0{,}05\%$	
HR:	532 nm	$r^2 > 99{,}90\%$	
	1064 nm	$r^2 > 99{,}97\% \pm 0{,}02\%$	

Berechnet man diese mit den Parametern aus ⇝Tabelle (5.1) gemäß

$$\mathcal{F} = \frac{\pi (r_1^2 r_2^2)^{1/4}}{1 - (r_1^2 r_2^2)^{1/2}} \quad , \tag{5.1}$$

so erhält man die Werte $\mathcal{F}_{1064} = 114 \pm 9$ und $\mathcal{F}_{532} = 3{,}2 \pm 0{,}24$.

Der Anforderung der Phasenanpassung zwischen fundamentalem und frequenzverdoppeltem Feld (Kapitel 3) wurde Rechnung getragen, indem der nichtlineare Kristall zwischen zwei Peltierelementen (Typ TEC1M-9.1-9.9-4.3/76 von EURECA Messtechnik GmbH) untergebracht wurde. Mit einem Tempertursensor (Hygrosens® Präzisions Temperatursensor SEMI 833 ET) konnte nun eine effektive Regelung aufgebaut werden (die gegenüber früheren Konstruktionen mit Heizwiderständen [Fra03] den Vorteil bietet, sowohl symmetrisch arbeiten zu können, als auch eine höhere Regelbandbreite aufzuweisen). Versuche haben ergeben, dass die Phasenanpassungstemperatur für den verwendeten Kristalltyp bei ca. 60 °C liegt (die Phasenanpassungstempertur ist stark von der Dotierung des Kristallmaterials abhängig). Weitere technische Details zur mechanischen Konstruktion der OPAs kann man der ⇝Abbildung 5.2 entnehmen.

Das Kontrollfeld (1064 nm) wurde zunächst durch einen elektrooptischen Modulator (EOM) transmittiert, dabei mit einer Phasenmodulation versehen (15 MHz im Fall von OPA1, 30 MHz für OPA2) und mittels zweier Linsen an die Eigenmode des Resonators angepaßt. Die Erfahrung hat gezeigt, dass diese Anordnung sensitiv für die Ausbildung parasitärer Resonatoren ist. Ein sol-

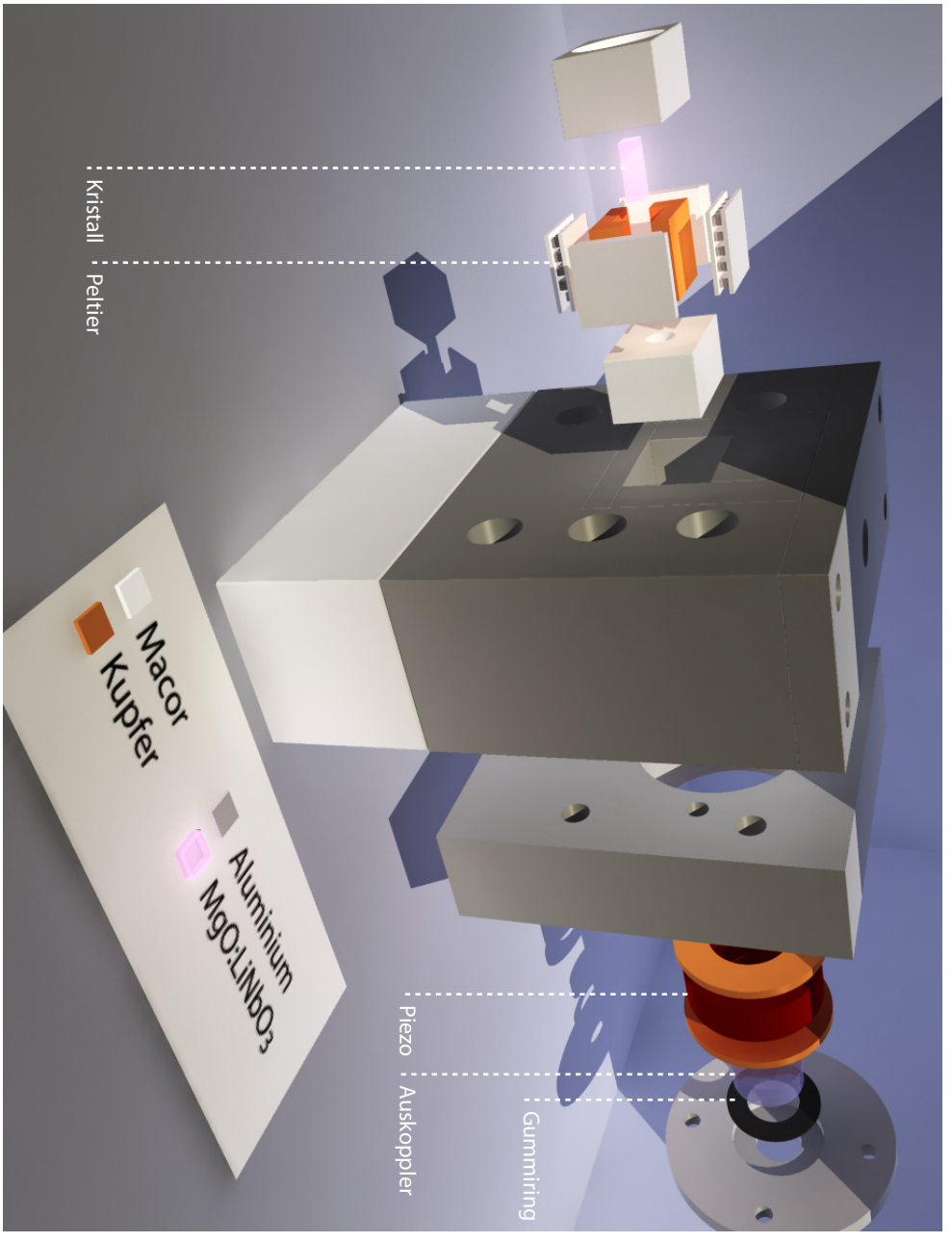

Abbildung 5.2 — Mechanische Konstruktion einer Quetschlichtquelle als Explosionsdarstellung. Befestigungen und elektrische Kontaktierung sind nicht gezeigt.

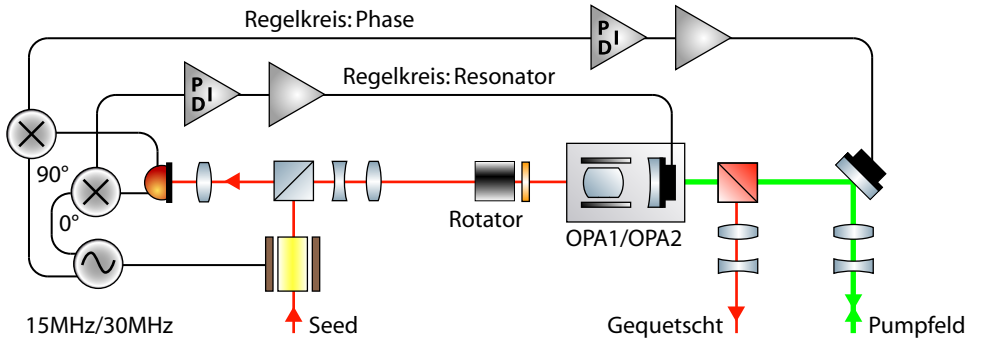

Abbildung 5.3 — Aufbau der Optik um einen OPA. Die Regelung eines OPAs wird mit 15 MHz betrieben, die des zweiten mit 30 MHz. Das Kontrollfeld (*„seed“*) dient der Längenregelung des OPA-Resonators und wird durch die HR-beschichtete Kristallseite eingestrahlt. In den längengeregelten Resonator wird durch die Auskoppelseite das Pumpfeld (532 nm) eingestrahlt. Fehlersignale für Seedfeld und Pumpfeld erhält man in Reflexion.

cher parasitärer Resonator driftet frei in seiner Länge, was zu unerwünschten Variationen der Stärke der Phasenmodulations-Seitenbänder führt. Diese machen sich wiederum unmittelbar im Gleichspannungsanteil der Fehlersignale bemerkbar, die in Reflexion der OPAs gewonnen werden und beeinträchtigen die Regelung durch Verschiebung des Arbeitspunktes massiv. Dieser Effekt wurde beseitigt, indem unmittelbar vor den OPAs je ein Faraday-Rotator mit Polarisator („optische Diode“) eingebracht wurde. Die geringe Baugröße der Rotatoren war dabei von Vorteil.

Auf der Auskoppelseite des Resonators wurden reflektiertes Pumpfeld (532 nm) und das aus dem Resonator stammende Feld durch einen dichroitischen Strahlteiler voneinander getrennt.

Führt man dieses Feld bei geregelter Resonatorlänge und auf Amplituden-Abschwächung geregelte Phase des Pumpfeldes einer Homodyndetektion zu, kann man bei einer Seitenbandfrequenz von 7 MHz die in Abbildung 5.4 wiedergegebene Messung gewinnen, die als typisches Leistungsverhalten der OPAs angegeben wird. Als Referenz gewinnt man zunächst die Varianz des Vakuumrauschens, indem man eine Messung bei geblocktem Signalstrahl durchführt. Typischerweise liefern die beiden OPAs eine nichtklassische Rauschunterdrückung von 5 dB.

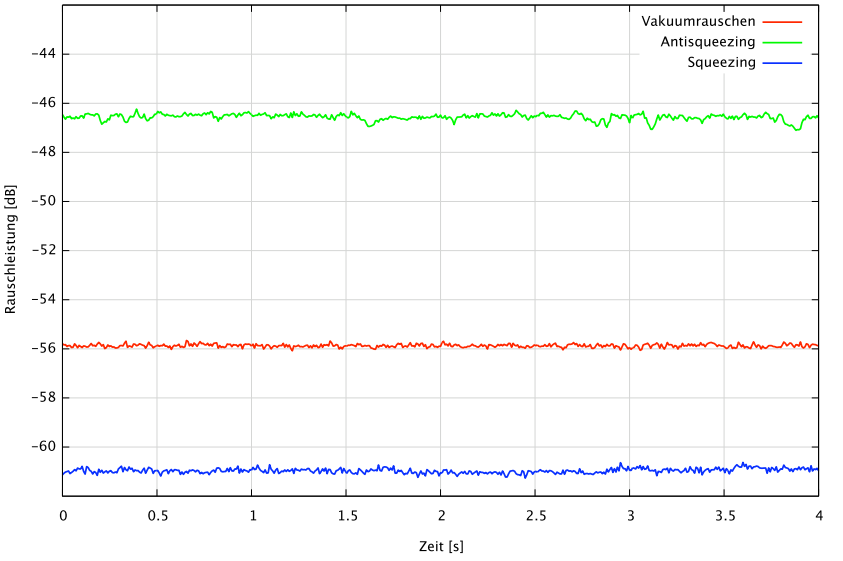

Abbildung 5.4 — Charakterisierung von OPA1. Dargestellt ist eine Messung bei einer Seitenbandfrequenz von 7 MHz von 4 s Dauer. Die Varianz des Vakuumrauschens ist als Referenz als rote Kurve eingetragen. Man erkennt die nichtklassische Rauschunterdrückung unterhalb des Vakuumrauschens (Squeezing (blau)) und das vergrößerte Rauschen der orthogonalen Quadratur (Antisqueezing (grün)), wobei jeweils auf die gequetschte, bzw. antigequetschte Quadratur geregelt wurde. Man liest eine nichtklassische Rauschunterdrückung von etwa 5 dB ab. Parameter der Messung: VBW 30 Hz, RBW 300 kHz.

5.3 Übertragung

Der als Transmissions-Abschnitt bezeichnete Teil des optischen Aufbaus hatte den Zweck, eine Übertragung gequetscher Zustände über einen optischen Kanal beachtlicher Länge zu emulieren. Dies ist in einem realistischen Szenario etwa möglich, indem man optische Fasern verwendet. In einem solchen Übertragungsszenario ist es unumgänglich, dass die gequetschten Zustände durch zufällige Phasenfluktuationen beeinträchtigt werden. Solche Phasenfluktuationen wurden im Experiment erzeugt, indem jeder gequetschte Strahl an je einem piezogetriebenen Umlenkspiegel reflektiert wurde. Die beiden Piezos wurden dabei von zwei unabhängigen Spannungen getrieben, die die gewünschte Rauschcharakteristik aufwiesen. Dieses Rauschen wurde durch die resultierende, mikroskopische Spiegelverschiebung somit in ein

Phasenrauschen des optischen Feldes umgesetzt. Wie im Kapitel 7 gezeigt werden wird, spielt die genaue Form des Phasenrauschens für das Funktionieren von Purifikation keine Rolle. Es wurde jedoch versucht, das zugrunde liegende theoretische Modell experimentell möglichst genau nachzubilden. Dazu wurde mit einem LABVIEW-Programm in Echtzeit ein auf Zufallszahlen basierendes *weißes Rauschen* erzeugt. Bei jeder Frequenz wies dieses Rauschen (in Übereinstimmung mit der Theorie) eine gaußsche Gewichtung auf. Darüberhinaus wurde das Rauschen durch einen digitalen Filter auf ein Frequenzband von 1–5 kHz eingeschränkt. Es wird davon ausgegangen, dass in diesem Frequenzband die Transferfunktion der verwendeten Piezos in erster Näherung weiß ist. Prinzipiell könnte das Phasenrauschen auch mit EOMs erzeugt werden. Die Wahl des Frequenzbandes ist außerdem derart erfolgt, dass die untere Bandpassfrequenz größer ist, als die Regelbandbreiten der Regelungen im Detektionsabschnitt. Damit war sichergestellt, dass etwa die Phasenregelung der optischen Lokaloszillatoren diesem Phasenrauschen nicht folgen konnte.

Das Rauschen wurde über die Soundkarte eines PCs mit fester Rauschleistung ausgegeben und anschließend durch einen variablen Abschwächer in seiner Stärke kontrolliert. Ein großer Vorteil dieser Methode besteht in der Möglichkeit, die Stärke des Rauschens (quantifiziert durch die Standardabweichung) komfortabel zu charakterisieren.

5.4 Detektion und Purifikation

Die beiden gequetschten (und mit Phasenrauschen beliebiger Stärke) versehenen Strahlen wurden dann auf einem Strahlteiler modenangepaßt und phasengeregelt überlagert. Dieser Strahlteiler ist ein wesentlicher Bestandteil des Protokolls und wird fortan als „Purifikationsstrahlteiler“ oder BS_{PUR} bezeichnet.

Zur Detektion kommen die beiden Felder in den beiden Ausgängen des Purifikationsstrahlteilers. Dazu wurde für beide Strahlen jeweils eine Homodyndetektion durchgeführt (die beiden Homodyndetektoren werden mit HD1 und HD2 bezeichnet). Die Homodyndetektion als Werkzeug der Wahl zum Vermessen der Quantenrauscheigenschaften optischer Felder ist bereits mehrfach ausführlich beschrieben worden. Wir können uns also auf eine Besprechung des Prinzips beschränken.

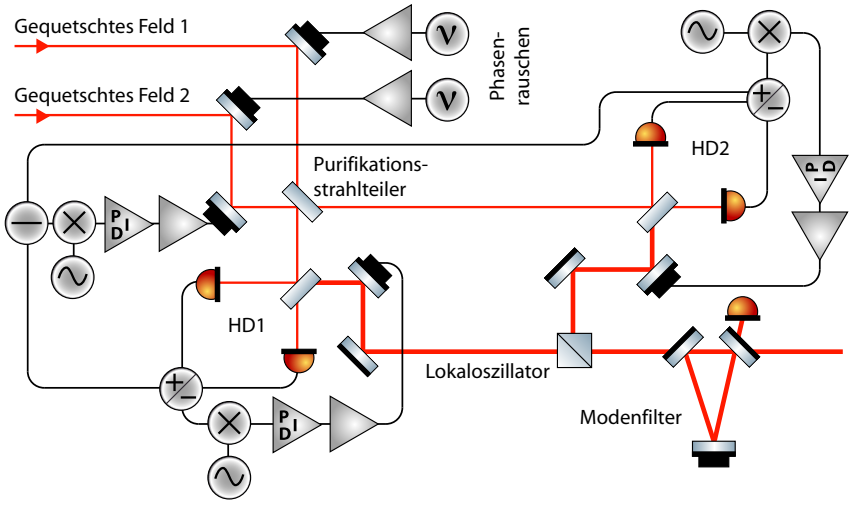

Abbildung 5.5 — Transmission und Detektion. Zwei piezogetriebene Planspiegel prägen den beiden gequetschten Feldern zufälliges, weißes, gaußsch gewichtetes Phasenrauschen (ν) auf. Diese beiden Felder werden auf einem Strahlteiler überlagert und die beiden Ausgänge dieses Strahlteilers mit je einem Homodyndetektor vermessen.

Bei der Homodyndetektion wird der zu vermessende Lichtstrahl mit einem leistungsstärkeren optischen Lokaloszillator phasengeregelt und modenangepasst auf einem Strahlteiler überlagert. Die beiden Ausgänge dieses Homodynstrahlteilers werden mit je einem Photodetektor registriert und die resultierenden Photoströme werden elektronisch voneinander subtrahiert. Man kann nun zeigen, dass die Rauscheigenschaften dieses Differenzstroms den Rauscheigenschaften des vermessenen Strahls entsprechen, wobei die kohärente Amplitude des Lokaloszillators als Verstärkungsfaktor eingeht. Wegen der Subtraktion spielen die Rauscheigenschaften des Lokaloszillators keine Rolle mehr. Ein Maß für die Güte der Überlagerunng ist die sogenannte Visibility $\mathcal{V}$. Diese ist experimentell leicht zugänglich, indem man den Lokaloszillator auf das Leistungsniveau des Signalfeldes abschwächt. Man betrachtet nun in einem Ausgang des Homodynstrahlteilers die durch Phasenschieben maximal erreichbare interferometrische Auslöschung ($I_{\min}$) und Verstärkung ($I_{\max}$). Daraus erhält man sofort die Visibility

$$\mathcal{V} = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \tag{5.2}$$

mit $0 \leq \mathcal{V} \leq 1$, wobei der Wert $\mathcal{V} = 1$ eine perfekte Modenanpassung bedeutet. Experimentell typische Werte lagen bei $\mathcal{V} = 0{,}984$ für HD1 und $\mathcal{V} = 0{,}987$ für HD2. Für das Erreichen hoher Visibilities ist die Modenqualität des Lokaloszillators mitentscheidend. Um diese zu Verbessern wurde der Lokaloszillator durch einen räumlichen Modenfilter in Form eines auf Resonanz geregelten Ringresonators ($\mathcal{F} = 10500$) transmittiert. Damit konnten die erreichbaren Visibilities deutlich verbessert werden. Hohe Visibilities sind bei allen Experimenten mit gequetschtem Licht wichtig, da eine mangelhafte Modenanpassung unmittelbar als Verlustkanal wirksam wird.

Trägt der Signalstrahl (oder der Lokaloszillator) zusätzlich eine Phasenmodulation, so kann durch Demodulation ein Fehlersignal gewonnen werden, mit dem die Phase des Lokaloszillators auf dem Strahlteiler so geregelt werden kann, dass die Amplitudenquadratur des Signalstrahls vermessen wird. Exakt dieses Prinzip ist im hier vorgestellten Experiment realisiert worden.

Ist man an einer Untersuchung der Phasenquadratur interessiert, kann man die Gleichspannnungs-Differenz der beiden Photodetektoren betrachten. Diese stellt sofort ein Fehlersignal für die Phasenquadratur dar.

Soll eine beliebige Quadratur vermessen werden, kann ein von B. Hage ursprünglich für die Tomographie von Quantenzuständen entwickeltes Verfahren verwendet werden. Dazu generiert man ein Fehlersignal für eine beliebige Quadratur aus einer Linearkombination der Fehlersignale für die Amplituden- und Phasenquadratur.

Die beiden resultierenden Differenzphotoströme wurden dann nach Demodulation mit einem elektronischen Lokaloszillator bei 7 MHz mit einem Datenaufnahmesystem mit einer Frequenz von 100 kHz simultan digitalisiert. Anti-Aliasing-Filter wurden wie in Kapitel 6 dargestellt verwendet. Da lediglich die Rauschcharakteristiken bei einer Seitenbandfrequenz von 7 MHz betrachtet werden sollten, wurden die beiden Signale zuvor noch bei 7 MHz bandpassgefiltert.

Die Varianz des Vakuumrauschens erhält man als Referenz, indem man den Signalstrahl in jedem Homodyndetektor blockiert und somit die Rauschcharakteristik des Vakuumfeldes im Signaleingang vermisst.

5.5 Charakterisierung des Phasenrauschens

Das Phasenrauschen, welches die Effekte einer optischen Übertragung (etwa durch eine optische Faser) simulieren soll, wurde auf die beiden gequetsch-

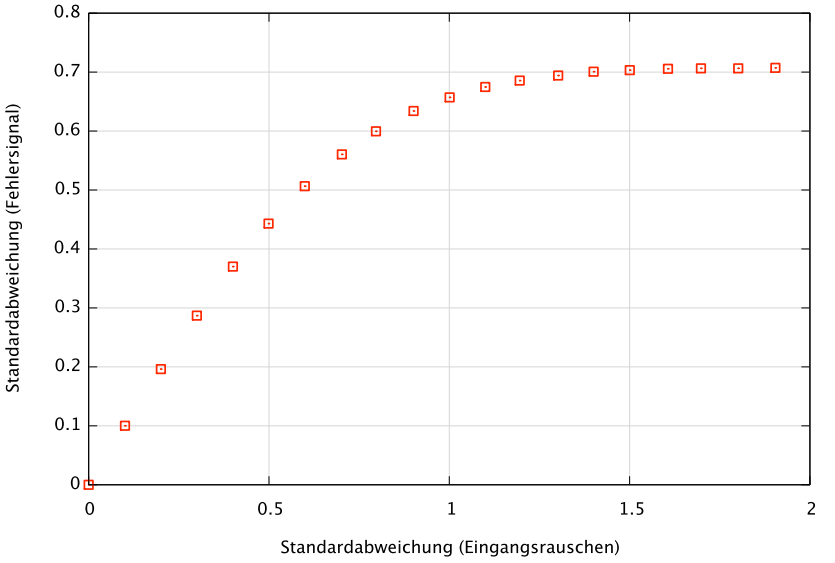

Abbildung 5.6 — Numerische Modellierung der Phasenrauscheichung. Dargestellt ist die Standardabweichung des sinusförmigen Fehlersignals über der Eingangsstandardabweichung. Das zugrunde liegende Fehlersignal hat in den dargestellten Einheiten eine Wellenlänge von 2π und eine Amplitude von 1.

ten Strahlen mittels zweier piezoaktuierter Umlenkspiegel aufgebracht. Das aufgebrachte Phasenrauschen soll dabei in seiner Stärke möglichst genau charakterisiert werden, das heißt, die Stärke des Rauschens (quantifiziert durch seine Standardabweichung) soll gegen eine als starr angenommene Referenzphase gemessen werden. Eine solche Referenzphase ist – per Definition – die optische Phase der Lokaloszillatoren, die für die Homodyndetektion verwendet wurden. Betrachtet man das Fehlersignal eines Homodyndetektors im geregelten Zustand (*closed loop*), so ist dieses (bis auf kleine Beiträge elektronischen Rauschens und Abweichungen durch Störungen, aus denen das Stellsignal generiert wird) gleich Null. Wird nun der Signalstrahl mit einem Phasenrauschen versehen, so wird dieses im Fehlersignal sichtbar, da die Rauschfrequenzen größer sind als die Regelbandbreite der Homodynregelung – das Rauschen des Fehlersignals ist ein unmittelbares Abbild des aufgebrachten Phasenrauschens.

Man muss hierbei beachten, dass das Fehlersignal eines Homodyndetektors die Form einer Sinus-Funktion hat, also nur in einem kleinen Bereich um den Arbeitspunkt linear ist. Dies führt dazu, dass die am Fehlersignal

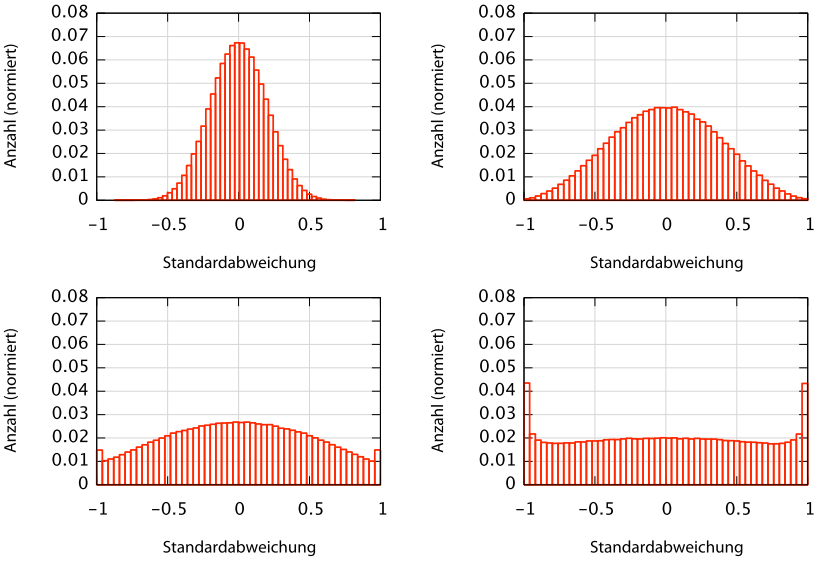

Abbildung 5.7 — Histogramme zur Eichung des Phasenrauschens. Dargestellt sind Standardabweichungen des Phasenrauschens von 0,2, 0,4, 0,6, 0,8. Man erkennt, wie sich für größere Standardabweichungen der sinusförmige Charakter des Homodyn-Fehlersignals offenbart.

zu messende Standardabweichung nicht für beliebig großes Phasenrauschen linear mit dem Eingangssignal variieren kann. Vielmehr ist die maximal zu beobachtende Standardabweichung durch die Amplitude des Fehlersignals limitiert. Dieser Effekt kann numerisch leicht simuliert werden (⇝Abbildung 5.6). Betrachtet man von den aufgenommenen Zeitserien Histogramme für verschiedene Rauschstärken (⇝Abbildung 5.7) wird dies leicht verständlich: Ist das Phasenrauschen so groß, dass ein erheblicher Teil der auftretenden Phasenverschiebungen größer als $\pi/2$ ist und damit die Amplitude des Fehlersignals voll ausnutzt, konzentrieren sich die Messwerte im Bereich der Umkehrpunkte des Fehlersignals. Phasenfluktuationen, die erheblich größer sind als $\pi/2$ werden (durch die zyklische Natur des Fehlersignals) wieder auf kleinere Messwerte abgebildet. Das Histogramm der Messwerte weicht stark von einer gaußschen Verteilung ab und das aufgebrachte Phasenrauschen wird durch Angabe der Standardabweichung nicht mehr treffend charakterisiert.

Um nun zu einer Kalibration von aufgebrachter Rauschstärke (gemessen in beliebigen Einheiten) auf die Standardabweichung der Phasenfluktuatio-

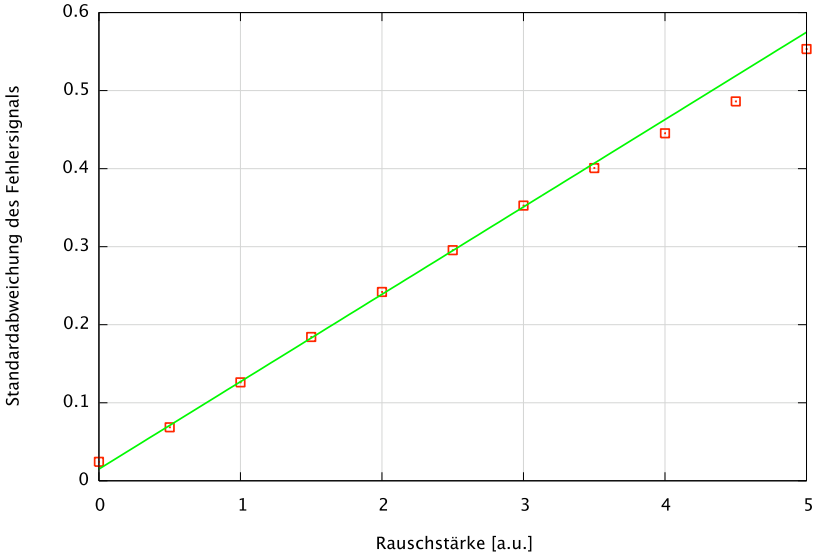

Abbildung 5.8 — Zur Eichung des Phasenrauschens. Die Standardabweichung ist über der Einstellung des Abschwächers (in Skaleneinheiten) aufgetragen. Für große Standardabweichungen entsteht eine Abweichung von der Linearität wie im Text beschrieben. Eine lineare Approximation für kleine Standardabweichungen liefert die Eichung des Abschwächers. Man erkennt weiterhin, dass die Eichkurve keine Ursprungsgerade ist. Die nicht verschwindende (allerdings kleine!) Streuung des Fehlersignals auch wenn kein zusätzliches Phasenrauschen aufgebracht wird resultiert aus elektronischem Rauschen und störungsverursachten Abweichungen des Fehlersignals aus denen das Stellsignal generiert wird.

nen zu gelangen, bewegt man sich im linearen Bereich des Fehlersignals. Für mehrere Werte der aufgebrachten Rauschstärke wird eine Zeitserie des Fehlersignals aufgenommen und bezüglich der Standardabweichung ausgewertet. Die beiden Größen werden gegeneinander aufgetragen (⇝Abbildung 5.8). An der Abbildung erkennt man den linearen Zusammenhang (vergleiche auch mit ⇝Abbildung 5.6). Man erkennt für große Werte des Eingangsrauschens bereits eine leichte Abweichung von der Linearität. Eine angepasste Gerade liefert die gewünschte Eichkurve zwischen aufgebrachter Rauschstärke und Standardabweichung des resultierenden optischen Phasenrauschens.

KAPITEL 6

Software

6.1 Softwareentwicklung mit Python

Einen wesentlichen Bestandteil der Experimente, die in dieser Arbeit dargestellt sind, bilden eine Reihe von Programmen und Routinen. Dabei kann man grob zwei Gruppen von Programmen unterscheiden: Zum Einen wurden theoretische Analysen in Form numerischer Simulationen vorgenommen, zum Anderen ist die zur Destillation von Quantenzuständen notwendige Nachselektierung als Software implementiert worden. Zusätzlich zu diesen beiden Gruppen gibt es eine Reihe von kleineren Hilfsprogrammen, die verschiedene Aufgaben bewerkstelligen und nicht eindeutig einer der beiden Gruppen zugeordnet werden können.

Das gesamte Softwarepaket, das in dieser Arbeit verwendet wurde, ist dabei in `Python` realisiert, einer Programmiersprache, die Anfang der 1990er Jahre in Amsterdam entwickelt wurde und zwischenzeitlich weite Verbreitung gefunden hat. Der Ansatz bei der Entwicklung von `Python` war der, eine möglichst übersichtlich zu programmierende und einfach zu begreifende Programmiersprache mit großem Funktionsumfang zu realisieren. Durch die stark reduzierte Syntax kann ein Programm fast wie übersichtlicher Pseudo-Code gelesen und verstanden werden. Gleichzeitig ist die Entwicklungszeit von Pythonprogrammen vergleichsweise kurz. Dies führt dazu, dass manche Programme, die in ihrer endgültigen Umsetzung in C++ oder Java implementiert werden sollen, zunächst in `Python` skizziert werden (*rapid-prototyping*).

Die häufig an einer Skriptsprache geäußerte Kritik der geringen Geschwindigkeit trifft auf `Python` nur eingeschränkt zu: Verwendet man etwa die Funk-

tionen des `numeric`-Paketes sinnvoll, kann `Python` durchaus mit MATLAB konkurrieren, was die Ausführungsgeschwindigkeit betrifft. Bestehen besondere Anforderungen an die Geschwindigkeit, können Subroutinen in anderen Sprachen maschinennah programmiert und von `Python` aufgerufen werden.

`Python` verfügt über eine dynamische Typenprüfung, d. h. es ist nicht nötig, den Typ einer Variablen bei deren Initialisierung explizit anzugeben, was die Programmierung in der Praxis weiter vereinfacht. Durch die Unnötigkeit, zu Kompilieren, können Veränderungen extrem schnell eingepflegt werden. Bei einfachen Anwendungen kann man dadurch komplett auf eine – sonst aufwändig zu erstellende – Benutzerschnittstelle verzichten und zum Beispiel Parameter direkt im Quellcode verändern.

6.2 Digitale Signalverarbeitung/Filter

Konzepte der digitalen Signalverarbeitung (*Digital Signal Processing*, DSP) spielen in der vorliegenden Arbeit an verschiedenen Stelle eine herausragende Rolle. Aus diesem Grunde sollen die zugrunde liegenden Konzepte und die benötigten Anwendungen kurz dargestellt und erklärt werden. Von besonderer Wichtigkeit sind dabei digitale Filter.

6.2.1 Periodische Sequenzen

Die Aufgabe digitaler Signalverarbeitung liegt in der Analyse physikalischer Prozesse. Als Beispiel dient eine zeitlich veränderliche Spannung, deren Amplitude kontinuierlich einen beliebigen Wert annehmen kann. Ein solches Signal bezeichnet man häufig als *analoges Signal*. Diese Bezeichnung entstammt der Frühzeit rechnergestützter Datenverarbeitung (vor 1980). In diesem Zeitraum konnten Differentialgleichungen gelöst werden, indem diese durch elektronische Baugruppen (Integratoren, Differenzierer, etc.) nachgebildet wurden. Eine Spannung in dieser Elektronik war dann *analog* zu einer Variablen der Differentialgleichung. Die Bezeichnung *analoges Signal* ist angesichts heutiger Anwendungen im Grunde nicht mehr richtig – man sollte vielmehr von einem *kontinuierlichen Signal* sprechen. Ein kontinuierliches Signal wird mit dem Symbol $X(t)$ bezeichnet.

Bei einem *digitalen Signal* ist im Gegensatz dazu die Zeitvariable quantisiert, was bedeutet, dass die Amplitude des Signals nur zu bestimmten Zeiten bekannt ist. Weiterhin ist im Allgemeinen auch die Amplitude diskretisiert. Ein Wertepaar bestehend aus einem diskreten Zeitwert und einem diskreten

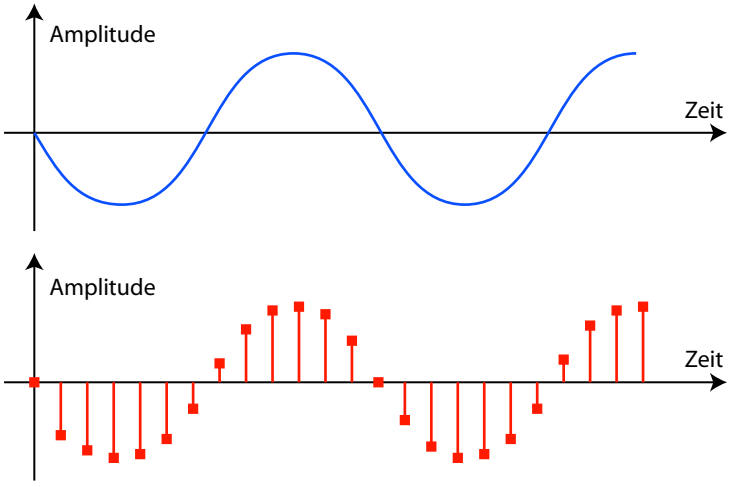

Abbildung 6.1 — Ein kontinuierliches Signal bei einer Frequenz ω und ein diskretes Signal. Obwohl man versucht ist, dem diskreten Signal ebenfalls die Frequenz ω zuzuordnen, werden wir sehen, dass dies nicht ohne weiteres möglich ist.

Amplitudenwert wird *sample* genannt. Wir bezeichnen ein digitales Signal mit dem Symbol $x(n)$, wobei n eine positive ganze Zahl ist, die die *samples* durchnummeriert.

6.2.2 Periodisches Sampling

Periodisches Sampling bedeutet die Darstellung eines kontinuierlichen (im Allgemeinen zeitabhängenden) Signals als Abfolge diskreter Werte mit konstantem zeitlichen Abstand. Man erreicht dies, indem man das kontinuierliche Signal mittels eines Analog/Digital-Konverters umwandelt und den Ausgang des Konverters erfasst. Dabei stellt sich zum Beispiel die Frage, mit welcher Geschwindigkeit dieses Sampling vollzogen werden muss, bzw. wie gut ein digitales Signal die Information, die im kontinuierlichen Ursprungssignal enthalten war, repräsentiert.

6.2.3 Aliasing: Doppeldeutigkeit

Um die „Doppeldeutigkeit“ eines digitalisierten Signals zu beschreiben, betrachtet man zunächst ein kontinuierliches Signal, welches die Form einer

Sinus-Schwingung mit irgend einer Frequenz f_0 besitzt:

$$X(t) = \sin(2\pi f_0 t). \tag{6.1}$$

Dieses Signal soll nun mit einer *Digitalisierungs-* oder *Sampling-Frequenz* f_s digitalisiert werden. Die Digitalisierung erfolgt also in gleichmäßigen Zeitschritten t_s, wobei $t_s = f_s^{-1}$. Der Wert des n-ten Samples beträgt folglich

$$x(n) = \sin(2\pi f_0 n t_s). \tag{6.2}$$

Bekanntlich ist nun die Sinus-Funktion periodisch bei Verschiebungen um ein ganzzahliges Vielfaches von 2π. Es ist also

$$\begin{aligned} x(n) = \sin(2\pi f_0 n t_s) &= \sin(2\pi f_0 n t_s + 2\pi m) \\ &= \sin\left(2\pi\left(f_0 + \frac{m}{n t_s}\right) n t_s\right). \end{aligned} \tag{6.3}$$

Nimmt man weiter an, dass m ein Vielfaches von n ist, also $m = kn$, kann man das Verhältnis m/n ersetzen:

$$x(n) = \sin\left(2\pi\left(f_0 + \frac{k}{t_s}\right) n t_s\right). \tag{6.4}$$

Ersetzt man noch t_s durch f_s^{-1} erhält man durch Vergleich:

$$x(n) = \sin(2\pi f_0 n t_s) = \sin(2\pi(f_o + k f_s) n t_s). \tag{6.5}$$

Bei ⇝Gleichung (6.5) handelt es sich um eine der wichtigsten Gleichungen auf dem Gebiet der digitalen Signalverarbeitung – ihre Konsequenzen sind weitreichend. Die ⇝Gleichung (6.5) bedeutet, dass eine Sequenz $x(n)$, die die digitale Repräsentation einer Sinus-Schwingung mit Frequenz f_0 ist, ebenso alle Schwingungen mit Frequenzen $f_0 + k f_s$ repräsentiert. Anders herum heißt dies, dass beim Vorliegen einer Sequenz $x(n)$ keine Möglichkeit besteht, herauszufinden, ob diese von einer Schwingung der Frequenz f_0 oder irgendeiner anderen Schwingung mit einer der Frequenzen $f_0 + k f_s$ erzeugt worden ist. Man betrachte etwa die ⇝Abbildung 6.3, in der verdeutlicht wird, dass eine Reihe von Datenpunkten, die mit einer Samplingfrequenz von 6 kHz digitalisiert wurden, ebenso zu einer Schwingung mit 1 kHz, wie zu einer mit 7 kHz gehören kann. Man spricht in diesem Zusammenhang von *Aliasing*. Nehmen wir nun an, dass wir uns für ein Frequenzband interessieren, dass

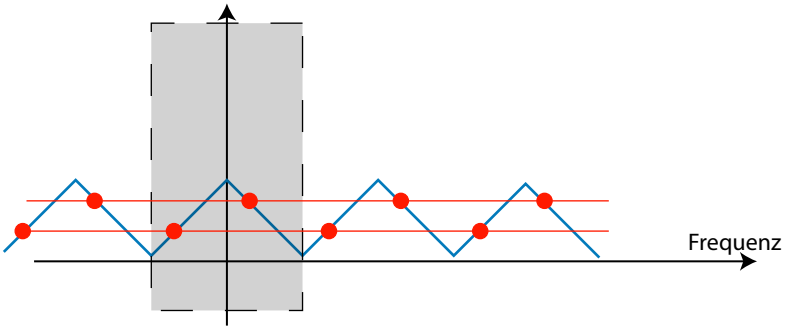

Abbildung 6.2 — Sogenannte „Haifischzahn-Abbildung“ zur Verdeutlichung des Aliasing-Effektes. Alle Frequenzanteile bei den Schnittpunkten einer Horizontalen mit den Flanken finden sich durch Aliasing im interessierenden Frequenzband (grau) wieder.

sich von $-f_s/2$ bis $f_s/2$ erstreckt. In diesem Fall lautet die Frage also, welche Frequenzanteile aufgrund von Aliasing in diesem Band wiederzufinden sind.

Eine instruktive Visualisierung ist die in ⇝Abbildung 6.2 gezeigte, sogenannte Haifischzahn-Darstellung, mit deren Hilfe die Antwort auf diese Frage leicht abgelesen werden kann. Die Spitzen des Musters liegen bei ganzzahligen Vielfachen der Samplingfrequenz f_s. Als Effekt des Aliasings kann abgelesen werden, dass ein Frequnzanteil an einem Schnittpunkt einer horizontalen Linie und einer Flanke des Dreieckmusters auf alle anderen Schnittpunkte abgebildet wird. Dieser Effekt muß bei allen praktischen Anwendungen, die eine digitale Datenerfassung beinhalten, bedacht werden.

Eine naheliegende Möglichkeit, dem Aliasing-Effekt zu begegnen, besteht darin, von vorn herein sicherzustellen, dass das zu digitalisierende Signal schlicht keine Anteile besitzt, die sich bei Frequenzen oberhalb der halben Digitalisierungsfrequenz befinden. Dies kann etwa durch Tiefpassfilterung bewerkstelligt werden, wobei die Unterdrückung des Filters im Stoppband hinreichend groß sein muss. Ein solcher Tiefpassfilter wird dann angesichts der Funktion als *Anti-Aliasing-Filter* bezeichnet. In der Praxis ergeben sich dabei oft Schwierigkeiten, einen Filter mit geeigneter Charakteristik zu konstruieren. Sollen mehrere Kanäle digitalisiert werden, ist man außerdem noch daran interessiert, die unterschiedlichen Filter in den einzelnen Kanälen identisch auszuführen.

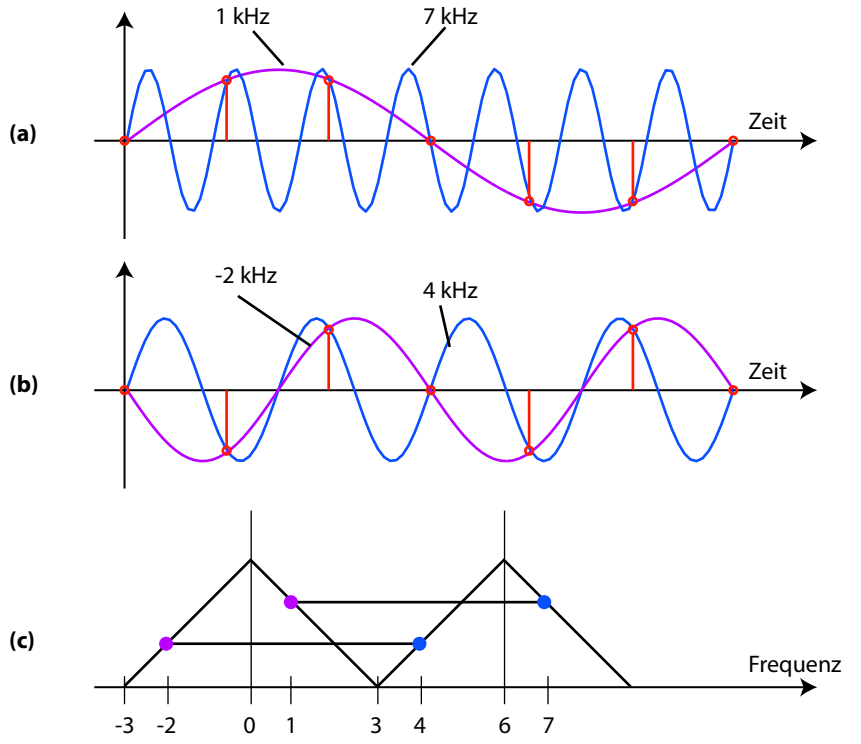

Abbildung 6.3 — Illustration des Aliasing-Effekts. In (a) wird eine Schwingung bei 7 kHz mit einer Samplingfrequenz von 6 kHz gesampled. In (b) wird mit derselben Samplingfrequenz eine Schwingung bei 4 kHz gesampled. Teil (c) der Abbildung verdeutlicht das Aliasing über einer Frequenzachse.

6.2.4 Erfassung tiefpassgefilterter Signale

Wir betrachten nun die Digitalisierung eines Signals, welches tiefpassgefiltert wurde, im Frequenzraum also lediglich Anteile im Frequenzband $-B < f < B$ besitzt (⇝Abbildung 6.4). Außerhalb dieses Bandes soll die Signalstärke idealerweise Null sein, mindestens jedoch kleiner als die Empfindlichkeit des Messsystems. Der obere Teil der Abbildung zeigt das Spektrum eines kontinuierlichen Signals. Man beachte, dass ein solches Spektrum eines bandlimitierten Signals von einem digitalen Signal nicht repräsentiert werden kann! Erfasst man ein Signal mit einem solchen Spektrum nun mit einem A/D-Konverter und einem Datenaufnahmesystem, indem man mit einer Sampling-Frequenz f_s digitalisiert, tritt der Effekt der Replikation auf, so wie in ⇝Abbildung

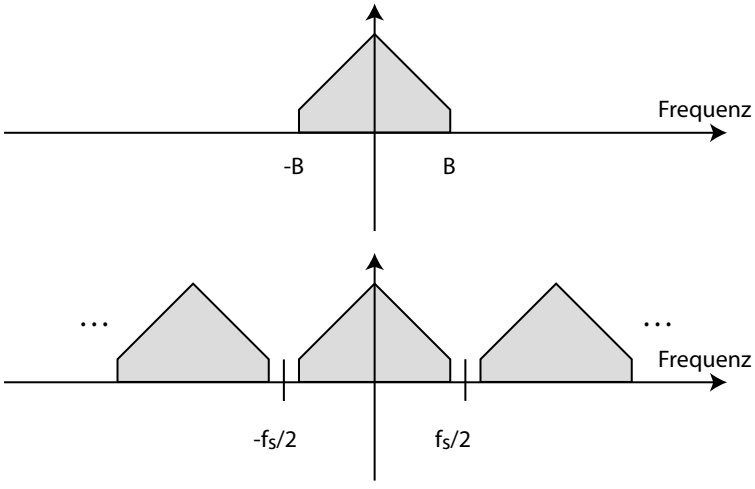

Abbildung 6.4 — Zur Digitalisierung eines tiefpassgefilterten Signals. Das Spektrum des Signals soll wie im oberen Teil der Abbildung gezeigt durch einen geeigneten Tiefpassfilter mit Eckfrequenz B eingeschränkt worden sein. Durch die Digitalisierung mit einer Frequenz f_S tritt (unten) der Effekt der Replikation auf, das heißt, das erfasste Signal kann nicht mehr ohne Weiteres einer bestimmten Frequenz zugeordnet werden.

6.4 (unterer Teil) dargestellt: Der diskretisierten Abfolge von Zahlen kann nicht mehr eindeutig angesehen werden, zu welcher der Frequenzen $f + kf_s$ sie gehört! Einzig die Kenntnis darüber, dass das Ausgangssignal auf ein Frequenzband eingeschränkt war (oder durch einen Tiefpass-Filter derart präpariert worden ist), schafft Klarheit.

Wird die Digitalisierungs-Frequenz zu klein gewählt (⇝Abbildung 6.5), dann kommt es zu einer Überschneidung der Replikate mit dem interessierenden Frequenzband (*undersampling*). Aus den Abbildungen kann man unmittelbar herauslesen, dass für die Digitalisierungs-Frequenz gelten muss:

$$f_s \geq 2B \tag{6.6}$$

Dieses sogenannte *Nyquist-Kriterium* in Kombination mit einem (analogen) Tiefpassfilter mit Eckfrequenz B (und hinreichend großer Unterdrückung im Stopband) stellt sicher, dass keine Aliasing-Effekte mehr auftreten. In der Praxis ist diese Tatsache inbesondere durch die endliche Unterdrückung jedes realen Filters begrenzt.

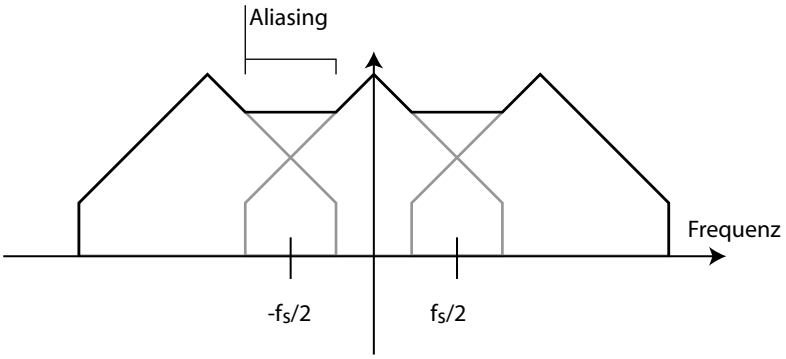

Abbildung 6.5 — Wird die Sampling-Frequenz f_S zu klein gewählt ($f_S < B/2$), so tritt wiederum Aliasing auf. Man liest aus der Abbildung heraus, dass die Eckfrequenz eines geeigneten Tiefpasfilters kleiner sein muss, als die halbe Sampling-Frequenz (=Nyquist-Frequenz).

In der Regel kennt man allerdings die Auflösung des Datenerfassungssystems (also die Anzahl der zur Verfügung stehenden, unterschiedlichen Werte für die Signalamplitude), so dass man den Filter derart gestalten kann, dass die im Stopband durchgelassenen Signale das *least significant bit* gerade nicht mehr ansprechen.

6.3 Digitale Filter

Die Aufgabe eines digitalen Filters besteht in der Entfernung von unerwünschten Signalanteilen oder der Extraktion gewollter Anteile (dies gilt in gleicher Weise für analoge Filter). Die im Folgenden betrachteten Filter sind solche, die auf Zeitserien angewendet werden. Es ist also nicht nötig, das Signal vor Anwendung des Filters einer Fouriertransformation zu unterziehen. Damit sind digitale Filter – bis auf Latenzzeiten – Echtzeitfilter (wiederum entsprechend einem analogen Filter).

In verschiedenen Anwendungen bieten digitale Filter eine Reihe von Vorteilen im Vergleich zu analogen Filtern:

1 | Digitale Filter liegen in Form eines Software-Codes vor. Sie sind damit relativ leicht zu verändern oder anzupassen. Im Fall analoger Filter sind dagegen ein sorgfältiges Neudesign und Änderungen an bestehender

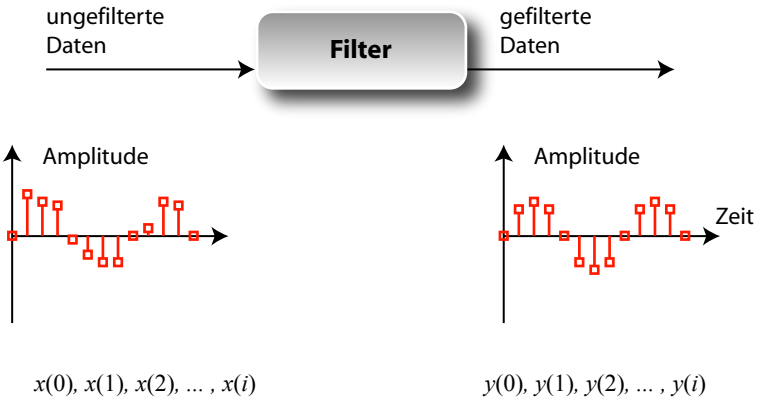

Abbildung 6.6 — Zum Prinzip eines digitalen Filters. Dieser setzt ein zeitdiskretes Eingabesignal $x(n)$ in ein zeitdiskretes Ausgabesignal $y(n)$ um.

Hardware notwendig. Das Design eines digitalen Filters ist auf jedem handelsüblichen PC problemlos möglich.

2 | Das Verhalten eines analogen Filters kann bestenfalls im Rahmen der Toleranzen der verwendeten elektronischen Bauteile vorhergesagt werden. Mithin müssen in der Regel zeitaufwendige Test- und Kalibrationsphasen (oft mehrmals) durchlaufen werden.

3 | Analoge Filter unterliegen Umwelteinflüssen, die das Verhalten verändern können (etwa Drift durch Veränderungen der Umgebungstemperatur).

4 | Mit digitalen Filtern ist es problemlos möglich, niedrige und sehr niedrige Frequenzen (mHz) zu bearbeiten. Mit zunehmender Rechengeschwindigkeit wird der Frequenzbereich, in dem digitale Filter eingesetzt werden können, zunehmend auch nach oben hin erweitert.

5 | Es ist möglich, digitale Filter zu konstruieren, die sich adaptiv – etwa an gewisse Charkteristika des Signals – anpassen können.

Zur Verdeutlichung der Funktionsweise eines digitalen Filters betrachten wir ein analoges Signal $X(t)$, etwa einen zeitlichen Spannungsverlauf. Wird

dieses Signal mit einer Samplingzeit $t_s = f_s^{-1}$ digitalisiert, resultieren daraus *samples*

$$x(0), x(1), x(2), \ldots, x(i) \quad \text{mit} \quad x(n) = X(nt_s), \tag{6.7}$$

die etwa im Speicher eines Rechners vorliegen. Man beachte, dass die zukünftigen Samples $x(i+1)$, $x(i+2)$ zum Zeitpunkt $t = it_s$ natürlich noch nicht zur Verfügung stehen. Diese Reihe von Samples steht nun einem digitalen Filter zur Verfügung, der, einer Rechenvorschrift folgend, daraus eine neue Reihe von Samples

$$y(0), y(1), y(2), \ldots, y(i) \tag{6.8}$$

generiert. Die Wirkungsweise des Filters wird dabei von der genauen Form der Rechenvorschrift bestimmt.

Wir betrachten nun exemplarisch eine Reihe einfacher Filter, die beispielhaft das Funktionieren digitaler Filter illustrieren sollen.

1 | Unity Gain Filter: $y(n) = x(n)$. Hierbei handelt es sich um den einfachst denkbaren Filter, bei dem jedes Ausgabesample exakt dem Eingabesample gleicht.

2 | Gain Filter: $y(n) = Kx(n)$. Für eine konstante Zahl K wirkt dieser Filter als Verstärker, wobei jedes *sample* mit K multipliziert wird. (Für Werte $K < 1$ wirkt der Filter folglich als Abschwächer).

3 | Verzögerungsfilter $y(n) = x(n-1)$. Der Ausgabewert zum Zeitpunkt $t = nh$ entspricht dem Eingabewert zu einem früheren Zeitpunkt $t = (n-1)h$. Das Signal wird durch den Filter also um die Zeit h verzögert. Man beachte, dass der erste Ausgabewert $y(0)$ nicht definiert ist, da kein Eingabewert $x(-1)$ existiert. Gewöhnlich nimmt man bei der Implementation eines solchen Filters an, dass alle Eingabewerte zu Zeitpunkten $t < 0$ gleich Null sind.

4 | Paar-Differenz-Filter $y(n) = x(n) - x(n-1)$.

5 | Paar-Mittel-Filter $y(n) = (x(n) + x(n-1))/2$.

6 | Zentral-Differenz-Filter $y(n) = (x(n) - x(n-2))/2$.

Als *Ordnung* eines Filters bezeichnet man die Anzahl der vorangegangenen *samples* $x(i)$, die jeweils gespeichert werden müssen, um einen Ausgabewert zu berechnen. Demnach ist etwa die Ordnung des Unity Gain Filters gleich Null (es wird kein *vorangegangenes sample* benötigt), die des Paar-Mittel-Filters gleich Eins. Die Ordnung des Zentral-Differenz-Filters ist dagegen

gleich Zwei, denn es müssen zwei vorangegangene Eingangswerte ($x(n-1)$ und $x(n-2)$) gespeichert werden.

6.3.1 FIR und IIR

Allen genannten Beispielen gemein ist die Tatsache, dass zur Berechnung eines Ausgabewertes lediglich eine gewisse Zahl vorangegangener Eingabewerte benötigt wird. Einen Filter dieser Art bezeichnet man als *finite impulse response* (FIR) Filter oder auch als *nicht-rekursiven* Filter. Im Gegensatz dazu steht der *rekursive* Filter (*infinite impulse response*, IIR), bei dem zusätzlich zu den Eingabewerten *frühere Ausgabewerte* benutzt werden, um den Wert eines *samples* zu berechnen.

Die Bezeichnungen rühren daher, dass die Impulsantwort eines solchen IIR-Filters (ein Impuls ist etwa gegeben durch ein Eingangssignal der Form $x(0) = 1, x(i) = 0$ für $i > 0$) theoretisch unendlich lange anhält. Tatsächlich ist es so, dass die Impulsantwort eines realistischen Filters innerhalb einer endlichen Zeit auf praktisch Null abfällt. Instruktiver sind daher die Bezeichnungen *nicht-rekursiv* und *rekursiv*.

Ein Beispiel für ein IIR-Filter ist etwa der Filter

$$y(n) = x(n) + y(n-1). \tag{6.9}$$

Um die Wirkung dieses Filters verstehen zu können, macht es Sinn, die ersten Ausgabewerte aufzuschreiben (man nimmt wieder an, dass die Eingabewerte $x(i)$ für $i < 0$ gleich Null sind):

$$\begin{aligned} y(0) &= x(0) + y(-1) = x(0), && (6.10)\\ y(1) &= x(1) + y(0) = x(0) + x(1), && (6.11)\\ y(2) &= x(2) + y(1) = x(0) + x(1) + x(2), && (6.12)\\ y(3) &= x(3) + y(2) = x(0) + x(1) + x(2) + x(3). && (6.13) \end{aligned}$$

Ein Ausgabewert dieses Filters besteht also aus der Summe *aller* vorhergehenden Eingabewerte. Dieses Beispiel illustriert einen großen Vorteil von rekursiven Filtern. Während die Implementation dieses Filters als nicht-rekursivem Filter es erfordert, alle vorhergehenden Eingabewerte zu speichern, benötigt der rekursive Filter lediglich einen einzigen Wert. Man verallgemeinert sinnvollerweise die Definition der *Ordnung* eines Filters für den Fall rekursiver Filter: Die Ordnung eines rekursiven Filters ist entweder die Anzahl benötigter früherer Eingabewerte oder die Anzahl der benötigten früheren Ausgabewerte, je nachdem, welche von beiden größer ist. Daraus folgt, dass ein rekursiver Filter mindestens die Ordnung Eins hat.

6.3.2 Filterkoeffizienten und Transferfunktion

Ein allgemeiner rekursiver Filter kann in der symmetrischen Form

$$b_0 y(n) + b_1 y(n-1) + \ldots b_j y(n-j) = a_0 x(n) + \ldots + a_k x(n-k), \quad (6.14)$$

die äquivalent zu der Darstellung

$$y(n) = \frac{1}{b_0}\left[a_0 x(n) + \ldots + a_k x(n-k) - b_1 y(n-1) - \ldots b_j y(n-j)\right] \quad (6.15)$$

ist, aufgeschrieben werden. Die Koeffizienten b_i nennt man *feedback*-Filterkoeffizienten, denn sie bestimmen die Art und Weise der Rückkopplung vorhergehender Ausgabewerte auf den aktuell zu generierenden Ausgabewert. Entsprechend werden die Koeffizienten a_i als *feedforward*-Koeffizienten bezeichnet. Manchmal benennt man demzufolge k als *feedforward*-Ordnung und j als *feedback*-Ordnung des Filters.

Wir benötigen noch den Verzögerungsoperator z^{-1}, der auf ein *sample* in der folgenden Art und Weise wirkt:

$$z^{-1} x(n) = x(n-1). \quad (6.16)$$

Wendet man also diesen Operator auf einen Eingabewert an, so erhält man den vorangegangenen Eingabewert. In gleicher Weise wirkt der Operator auf Ausgabewerte. Man definiert sinnvollerweise die Mehrfachanwendung dieses Operators durch

$$\underbrace{z^{-1} \cdots z^{-1}}_{p\text{-mal}} x(n) = z^{-p} x(n) = x(n-p). \quad (6.17)$$

Die symmetrisierte Form der Darstellung des Filters kann auch als

$$\sum_{l=0}^{j} b_l y(n-l) = \sum_{m=0}^{k} a_m x(n-m) \quad (6.18)$$

geschrieben werden. Bildet man auf beiden Seiten die Z-Transformation, so erhält man mit dem Verzögerungsoperator die Form

$$\sum_{l=0}^{j} b_l z^{-l} Y(z) = \sum_{m=0}^{k} a_m z^{-m} X(z). \quad (6.19)$$

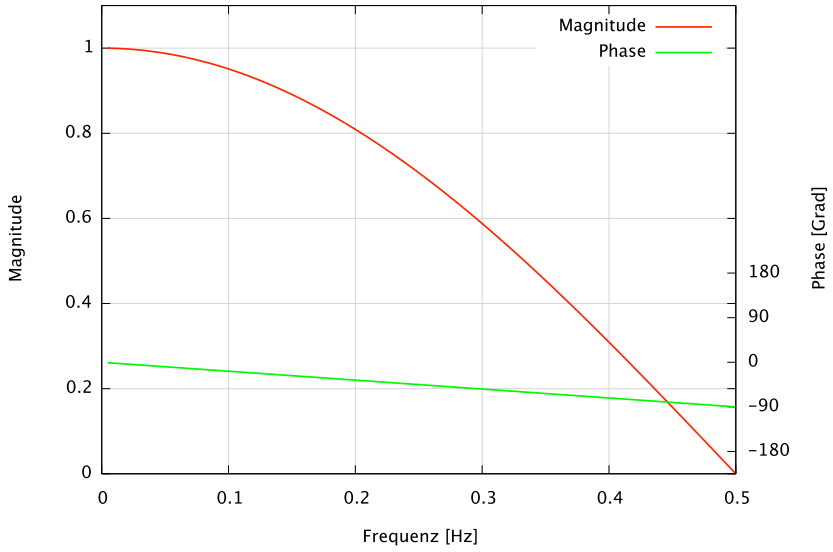

Abbildung 6.7 — Transferfunktion eines Paar-Mittel-Filters. Die Magnitude dieses Filters fällt bei der halben Sampling-Frequenz wie erwartet auf Null ab, während die Phase an dieser Stelle -90 Grad beträgt.

Damit definiert man die Transferfunktion des Filters

$$H(z) = \frac{Y(z)}{X(z)} = \frac{\sum_{m=0}^{k} a_m z^{-m}}{\sum_{l=0}^{j} b_l z^{-l}}. \tag{6.20}$$

Wir betrachten erneut den oben eingeführten Paar-Mittel-Filter, der durch $y(n) = 1/2(x(n) + x(n-1))$ beschrieben wird. Der Verlauf der Transferfunktion eines solchen Filters kann unmittelbar vorhergesehen werden: Im Fall eines konstanten Eingabesignals liefert der Filter auch ein konstantes Ausgabesignal mit Verstärkung Eins. Bearbeitet man allerdings ein Signal mit einer Frequenz, die der halben Digitalisierungsfrequenz (Nyquist-Frequenz) entspricht, so wird dieses Signal vom Filter vollständig ausgelöscht. Weiter kann man sich fragen, wie groß die Phasenverzögerung ist, die von diesem Filter eingeführt wird. Da die Magnitude des Filters das Mittel zwischen zwei aufeinander folgenden Eingabewerten ist, sollte sich diese Verzögerung ebenfalls in der Mitte zwischen zwei solchen Signalen befinden. Für ein Signal bei der halben Samplingfrequenz entspricht dies einer Verzögerung um eine Viertel Periode des Eingangssignals, entsprechend 90 Grad. Ein Blick

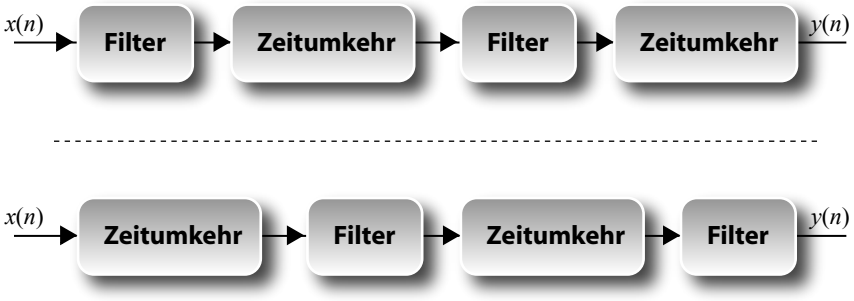

Abbildung 6.8 — Zwei Konzepte, wie ein Filter ohne Phasenverzerrung implementiert werden kann. Da der Prozess der Zeitumkehr nötig ist, kann das Verfahren nicht in Echtzeit angewendet werden.

auf die Transferfunktion des Filters (⇝Abbildung 6.7) bestätigt genau dieses Verhalten.

6.3.3 Filter ohne Phasenverzerrung

Typischerweise führen Filter, wie wir gesehen haben, einen nichtlinearen Phaseneffekt ein. Dieser ist manchmal nicht erwünscht oder sogar schädlich (Kapitel 7). Es ist allerdings möglich, einen IIR-Filter so zu konstruieren, dass keine nichtlinearen Phasenverzerrungen eingebracht werden. Derselbe Filter wird dabei zweimal verwendet, so wie in ⇝Abbildung 6.8 dargestellt. Es ist dazu nötig, eine Zeitumkehr einzuführen, also einen abgelegten Datenstrom in umgekehrter Reihenfolge zu lesen. Folglich ist es nicht möglich, dieses Verfahren in einer Echtzeitanwendung zu implementieren.

Um zu verstehen, wie das Verfahren funktioniert, betrachten wir eine beliebige spektrale Komponente eines Eingabesignals $x(n)$. Diese habe eine Phase α. Man nimmt nun an, dass ein verwendeter IIR-Filter eine zusätzliche Phase $-\beta$ einführt, so dass die spektrale Komponente nach Durchlaufen des Filters eine Phase $\alpha - \beta$ aufweist. Die erste Zeitumkehr wird diese Phase konjugieren und eine weitere zusätzliche Phase $-\gamma$ einbringen. Nach der Zeitumkehr beträgt die Phase der betrachteten spektralen Komponente also $-\alpha + \beta - \gamma$. Das zweite Durchlaufen des Filters wird erneut einen Phasensprung $-\beta$ verursachen, so dass nun eine Phase von $-\alpha - \gamma$ vorliegt. Erneute Zeitumkehr wird erneut konjugieren und wiederum eine Phase $-\gamma$ verursachen, so dass

nun die Gesamtphase $\alpha + \gamma - \gamma = \alpha$ vorliegt. Man vollzieht sofort nach, dass die Phase des Ausgabesignals $y(n)$ genau der Phase des Eingabesignals $x(n)$ gleicht, der Filter also einen Phasensprung von Null Grad über den gesamten Spektralbereich besitzt.

Eine äquivalente Realisierung eines solchen Filterprozesses ohne Phasenverzerrung ist in ⇝Abbildung 6.8 (unterer Teil dargestellt). Es bleibt dem Leser überlassen, zu prüfen, dass auch in dieser Anordnung keine Phasenverschiebung auftritt.

Nachteil dieser Methode ist die nicht gegebene Echtzeitfähigkeit – es handelt sich also um ein reines Nachbearbeitungsverfahren. Weiterhin wird bei jeder Anwendung des Filters erneut das Einschwingverhalten zu beachten sein, so dass im Allgemeinen eine gewisse Länge L zu Beginn des Datenstroms unbrauchbar wird. Weiter kann sich nachteilig auswirken, dass die Rauhigkeit des Passbandes eines solchen Filterprozesses doppelt so groß ist, wie die des einzelnen Filters. Ebenso wird die Unterdrückung im Stopband des Gesamtfilters halbiert.

6.4 Zufallszahlen

Die Simulationsroutinen zur Purifikation basieren im Wesentlichen auf langen Sequenzen von Zufallszahlen, die Sequenzen von Messwerten, die einer Quantenstatistik genügen, repräsentieren sollen. Es ist daher wichtig, sich darüber Klarheit zu verschaffen, wie es um die Qualität der verwendeten Zufallszahlen bestellt ist. Dabei steht die Frage im Vordergrund, wie *zufällig* die verwendeten Zufallszahlen tatsächlich sind – eine Frage, deren Beantwortung erstaunlich schwierig ist.

Ein verblüffend einfaches Verfahren zur analytischen Konstruktion einer Abfolge „zufälliger“ Zahlen wurde von John von Neumann 1946 vorgeschlagen. Seine Idee bestand darin, die jeweils nächste Zufallszahl einer Sequenz zu erzeugen, indem die vorhergehende Zahl quadriert und die mittleren Ziffern extrahiert werden. Verwendet man zum Beispiel Zahlen mit vier Ziffern und startet man mit der willkürlich gewählten Zahl 5743, so erhält man durch Quadrieren

$$32982049 \tag{6.21}$$

und die nächste Zahl der Reihe lautet 9820. Wie kann aber eine solche Sequenz, in der jede Zahl durch die Vorhergehende vollständig bestimmt ist, zufällig sein? Die Antwort lautet, dass eine solche Sequenz nicht zufällig *ist*, aber

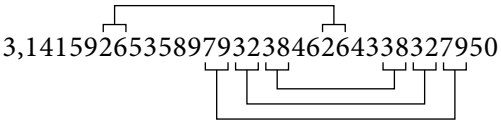

Abbildung 6.9 — Die ersten Stellen der Kreiszahl π und die Schwierigkeit der Kreiszahl, einen Zufallstest zu bestehen. Der erste Zifferpaarzwilling ist die 26. Der zweite Zwilling ist dabei völlig symmetrisch zwischen nicht weniger als drei weiteren Zifferpaarzwillingen eingebettet – obwohl in der Ziffernfolge der Kreiszahl alle Ziffern gleichverteilt auftauchen.

zufällig *erscheint*. Sequenzen dieser Art werden manchmal als *pseudozufällig* oder *quasizufällig* bezeichnet.

Betrachtet man lediglich das Ziehen einer einzigen Zahl, so ist es einfach, eine Definition zu formulieren bezüglich der Zufälligkeit dieser Zahl. Ein ungezinkter Würfel weist bekanntlich eine Wahrscheinlichkeit von 1/6 für das Zustandekommen jeder Augenzahl auf. Wirft man denselben Würfel sehr oft, erhält man eine Gleichverteilung als Statistik der Ergebnisse der Würfe.

Betrachtet man nun eine Abfolge (oder *Sequenz*) von Zufallszahlen, so muss man fordern, dass jede Zufallszahl von den anderen zustande gekommenen Zahlen statistisch unabhängig sein muss. Dies bedeutet, dass die Realisierung einer Zahl die Wahrscheinlichkeit nicht verändern darf, dass dieselbe Zahl erneut zustande kommt.

Eine endliche Sequenz von Zufallszahlen auf ihre Zufälligkeit zu testen ist nun daher besonders schwierig, da sich (wegen der Statistik der zustande kommenden Zufallszahlen) natürlich auch Sequenzen realisieren, die schon für das menschliche Auge keine Zufälligkeit aufzuweisen scheinen – etwa das fünfmalige „Würfeln einer 6“ in Folge. Man mache sich klar, dass das Zustandekommen der Sequenz 1, 4, 5, 2, 3, 6, 2, 1, 6, 3 genauso wahrscheinlich ist, wie das Zustandekommen der Sequenz 1, 1, 1, 1, 1, 1, 1, 1, 1, 1! Die letzgenannte Sequenz erscheint dabei nicht nur dem menschlichen Auge weniger zufällig, sie würde auch keinen statistischen Test (etwa auf Autokorrelation) bestehen: Man kann sich der Zufälligkeit einer gegebenen Sequenz niemals sicher sein. Es ist also niemals definitiv möglich, einen Nachweis zu führen, dass eine gegebene Sequenz von Zahlen zufällig zustande gekommen ist.

Man kann sich diesem Problem pragmatisch nähern, indem man *viele* Sequenzen von Zufallszahlen, die mit einem bestimmten Generator gewonnen wurden, testet. Wenn viele Sequenzen den Test nicht bestehen, ist zur Vorsicht

geraten.

Von Neumanns Methode ist, wie man sich leicht klar machen kann, kein besonders guter Zufallszahlengenerator, denn sie birgt die Gefahr, „hängen zu bleiben“, also einen kurzen Zyklus sich immer wiederholender Zahlen zu produzieren. Taucht etwa in der Sequenz die Zahl 0000 auf, wird sich diese immer fort reproduzieren.

Park und Miller [Par88] haben in ihrer grundlegenden Veröffentlichung darauf hingewiesen, dass die große Mehrheit der verfügbaren (und ständig verwendeten) Zufallszahlengeneratoren absolut unzureichend arbeitet.

Zwischenzeitlich existieren eine ganze Reihe zuverlässiger, statistischer Testverfahren, mit denen die Qualität von Sequenzen von Zufallszahlen geprüft werden kann. Ein sehr bekanntes und oft verwendetes Verfahren ist der sogenannte „Chi-Quadrat-Test“ (χ^2-Test). Die Funktionsweise kann an einem Beispiel erfasst werden. Man betrachtet das Werfen eines Paares ungezinkter Würfel. Stellt man die erzielte Augensumme s der Wahrscheinlichkeit des Auftretens dieser Augensumme p_s gegenüber, erhält man:

$$\begin{array}{rccccccccccc} s = & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ p_s = & \frac{1}{36} & \frac{1}{18} & \frac{1}{12} & \frac{1}{9} & \frac{1}{36} & \frac{1}{6} & \frac{1}{36} & \frac{1}{9} & \frac{1}{12} & \frac{1}{18} & \frac{1}{36} \end{array} \tag{6.22}$$

Wird das Würfelpaar n mal geworfen, erhält man das Ergebnis s im Durchschnitt np_s mal. In jeder Realisierung dieses Experimentes wird man jedoch Abweichungen von dieser Statistik erwarten.

Eine Möglichkeit, qualitativ festzustellen, ob die Würfel gezinkt sind, besteht in der Angabe der quadratischen Abweichung der beobachteten Anzahl von Ergebnissen Y_s von der erwarteten Anzahl np_s. Summiert man über diese Abweichungen, erhält man

$$V = (Y_2 - np_2)^2 + \cdots + (Y_{12} - np_{12})^2. \tag{6.23}$$

Gezinkte Würfel würden einen großen Wert für V liefern. Die Statistik V berücksichtigt jedoch alle Wurfergebnisse mit gleicher Gewichtung, ungeachtet der Tatsache, dass der Term $(Y_7 - np_7)^2$ einen höheren Beitrag liefern wird als etwa $(Y_2 - np_2)^2$. Dies ist durch Anpassen der Gewichtung leicht zu korrigieren:

$$V = \frac{(Y_2 - np_2)^2}{np_2} + \cdots + \frac{(Y_{12} - np_{12})^2}{np_{12}}. \tag{6.24}$$

Akzeptable Werte für V können für eine vorgegebene Vertrauenswahrscheinlichkeit bei bekannter Anzahl von Freiheitsgraden berechnet werden. Außerdem muss die Anzahl n der Würfe hinreichend hoch gewählt werden.

Neben diesem einfachen Verfahren existieren eine ganze Reihe zuverlässiger statistischer Testverfahren, mit denen die Qualität von Zufallszahlen geprüft werden können. Die wichtigsten lauten:

1 | Frequency Test

2 | Runs Test

3 | Binary Matrix Rank Test

4 | Spectral Test

5 | Non-Overlapping Template Matching Test

6 | Overlapping Template Matching Test

7 | Maurer's Universal Statistical Test

8 | Linear Complexity Test

9 | Serial Test

10 | Approximate Entropy Test

11 | Cumulative Sums Test

12 | Random Excursion Test

13 | Reverse Arrangements Test

14 | Chi-Square Test

15 | Diehard Test

Ebenso existiert inzwischen eine große Anzahl von Zufallszahlengeneratoren. Den meisten können Schwächen bezüglich der Qualität der Zufallszahlen nachgewiesen werden und viele erweisen sich bei genauer Betrachtung als unbrauchbar. D. Knuth rät in seinem Buch „The Art of Computer Programming" [Knu81]: *„. . . look at the subroutine library of each computer installation in your organization, and replace the random number generators by good ones."*

Erstaunlicherweise ist einer der besten Generatoren auch einer der am längsten bekannten: Obwohl der *Lehmer-Algorithmus* [Leh51] bereits 1951 entwickelt wurde, kann er nach wie vor den meisten statistischen Tests genügen.

Bei Lehmers Algorithmus handelt es sich um einen *linear congruentual generator* (LCG). Es scheint zunächst eine einfache Aufgabe zu sein, eine unvorhersehbare Reihe von Zahlen zu erzeugen. Es ist jedoch eine fundamental andere (und anspruchsvollere) Aufgabe, eine – für alle praktischen Belange – unendlich lange Reihe statistisch unabhängiger Zufallszahlen zu generieren (die möglicherweise zusätzlich eine Gleichverteilung über dem Intervall $[0, 1]$ aufweisen sollen). Die schlichte Unvorhersehbarkeit hat mit der Zufälligkeit der Zahlenreihe nicht viel zu tun. Obwohl Lehmers Algorithmus gewisse Schwächen aufweist, ist er in der Lage, eine praktisch unendlich lange Folge von Zahlen zu generieren, die allen gängigen statistischen Tests genügt (vorausgesetzt, die Parameter des Algorithmus werden entsprechend gewählt. Eine falsche Wahl dieser Parameter kann alles verderben, wie wir sehen werden).

Der hier exemplarisch betrachtete Spezialfall von Lehmers Algorithmus setzt die Wahl von lediglich zwei Parametern voraus:

1 | Dem Modulus m, eine große Primzahl

2 | Dem Multiplikator a, einer ganzen Zahl aus der Reihe $2, \ldots, m-1$

Der Algorithmus liefert dann eine Folge von ganzen Zahlen $z_1, z_2, z_3, \ldots$ zurück, die aus der rekursiven Rechenvorschrift

$$z_{n+1} = f(z_n) \tag{6.25}$$

gewonnen werden. Die *generating function* $f(z)$ ist dabei gegeben durch

$$f(z) = az \bmod m. \tag{6.26}$$

Offenbar muß die Rekursion mit einem Startwert, dem sogenannten *seed* z_1 gestartet werden. Der *seed* kann aus der Reihe $(1, 2, \ldots, m-1)$ frei gewählt werden.

Als optionaler Schrittt kann der Algorithmus abgeschlossen werden, indem man per Division durch den Modulus m auf das Einheitsintervall normiert:

$$u_n = z_n / m. \tag{6.27}$$

Man beachte, dass die Funktion $f(z)$ niemals Null werden kann, da m eine Primzahl ist. Damit wird verhindert, dass der Algorithmus ab irgendeinem Wert nur noch Nullen zurückliefert (vergleiche mit von Neumanns Methode der Quadrierung). Damit kommt allerdings der Wert $u = 0$ nicht vor. Ebenso

kann der Wert $u = 1$ nicht angenommen werden. Die kleinste Zahl, die der Algorithmus (inklusive Normierung) produzieren kann, ist $1/m$, der größte lautet $1 - 1/m$. Erstaunlich ist, dass dieser Algorithmus, *wenn* die Zahlen m und a richtig gewählt werden, eine sehr lange Sequenz von Zahlen zurückliefert, die durch statistische Tests nicht unterschieden werden können von einer Sequenz, die durch blindes Ziehen von Zahlen aus dem Vorrat $1, 2, \ldots, m-1$ gewonnen wird. Genau in diesem Sinne produziert der Algorithmus eine Reihe von Zufallszahlen. Tatsächlich sind keine „Zufallsprozesse" beteiligt. Für eine feste Wahl von m und a produziert die Anwendung desselben *seeds* jedes mal die gleiche Sequenz von Zahlen. Man bezeichnet Zahlensequenzen, die auf diese Weise gewonnen werden daher machmal als *pseudozufällig*.

Wir betrachten zur Illustration ein einfaches Beispiel, bei dem die *generating function* durch

$$f(z) = 6z \bmod 13 \tag{6.28}$$

gegeben ist. Wählt man als *seed* die Zahl $z_1 = 1$, so erhält man die Sequenz

$$1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1. \tag{6.29}$$

Die Folge der Zahlen ist periodisch in der angegeben Sequenz, da der ursprüngliche *seed* wieder auftaucht. Die Periodenlänge beträgt $m - 1 = 12$. Diese Sequenz allerdings ist durch keinen statistischen Test unterscheidbar von einer Sequenz, die durch blindes Ziehen aus dem Zahlenvorrat $1, \ldots, 12$ zustande kommt. Die angegebene Funktion $f(z)$ ist eine sogenannte *full period generating function*, was bedeutet, dass *jede* Wahl des *seeds* eine Sequenz der maximalen Länge 12 erzeugt, die der Definition einer Zufallszahlenreihe genügt. Wir wollen nun illustrieren, dass die Wahl des Multiplikators a extrem wichtig ist. Wählt man ihn zu 7, statt zu 6, so produziert die *generating function* für den *seed* $z_1 = 1$ die folgende Sequenz:

$$1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1. \tag{6.30}$$

Man beachte das entstandene Muster in der zweiten Hälfte der Sequenz. Wie wir zu Beginn dieses Abschnitts ausführten, kann natürlich auch diese Sequenz als Zufallszahlensequenz aufgefasst werden (ebenso, wie die Sequenz $\ldots, 1, 1, 1, 1, \ldots$). Dennoch scheint diese Sequenz *weniger zufällig*, mindestens aber *unbefriedigender* zu sein.

Wählt man den *seed* zu $z_1 = 5$, ist die resultierende Funktion $f(z)$ keine *full period generating function* mehr. Die entstehenden Sequenzen (etwa $1, 5, 12, 8, 1$) haben nur noch Länge 4. Ein solches Auftreten von kurzen Perioden will bei der Konstruktion eines Zufallszahlenalgorithmus unbedingt

vermieden werden. Der Lehmer-Algorithmus ist theoretisch durchdringend untersucht worden und es ist bekannt, dass für einen Modulus $m > 3$ *fast alle* Multiplikatoren a eine *full period generating function* hervorbringen.

Von Lehman selber vorgeschlagen und noch heute weit verbreitet ist die Wahl der Mersenne-Primzahl $2^{31} - 1 = 2147483647$ als Modulo.

Die Suche nach einem geeigneten Multiplikator a orientiert sich nun an drei Kriterien:

1 | Die Funktion $f(x) = az \bmod m$ soll eine *full period generating function* sein.

2 | Die entstehende Sequenz soll möglichst für alle *seeds hinreichend zufällig* erscheinen.

3 | Die Implementation auf gängigen Rechnern muss möglich sein.

Das dritte Kriterium wird verständlich, wenn man bedenkt, dass bei der Wahl realistisch großer Werte beachtet werden muss, dass die entstehenden großen Zahlen (etwa az) in Variablen ablegbar und arithmetisch bearbeitbar sein müssen. Der bereits 1969 gemachte Vorschlag $a = 7^5 = 16807$ hat weite Verbreitung gefunden. Es ist bekannt, dass die entstehende Funktion $f(z)$ eine *full period generating function* ist. Die resultierenden Zufallszahlen sind extensiv mit dutzenden Tests betrachtet worden und weisen hervorragende Zufälligkeit auf. Die größten entstehenden Zahlen az, die bei der Berechnung auftreten, erfordern 46 bit. Dies ist auch auf einem 32 bit Betriebssystem bei geschickter Programmierung möglich (eine naive Umsetzung, die die maximale Größe von Variablen nicht beachtet oder ungünstige Verfahren wählt, um den *overflow* abzufangen, ist allerdings zum Scheitern verurteilt). Die Rechenleistung, die von der Umsetzung gefordert wird, ist heute kein limitierender Faktor mehr.

Im Rahmen der vorliegenden Arbeit wird eine immens weiter entwickelte Version dieses Algorithmus verwendet. Zur Erzeugung der Zufallszahlen für die Simulation der Destillation und Purifikation von Quantenzuständen konnte praktischerweise auf die `random`-Funktion von `Python` zurückgegriffen werden. Diese basiert auf einem Mersenne-Twister-Verfahren, dessen hervorragende Eigenschaften vielfach belegt wurden. Dieser Generator ist erst 1997 entwickelt worden und verfügt über die kollossale Periode $2^{19937} - 1$ (dies entspricht etwa 10^{6000}) bei gleichzeitig beeindruckender Geschwindigkeit. Der Generator hat vielfach die stringentesten Tests bestanden, einschließlich des sogenannten „Diehard-Tests“. Wir präsentieren an dieser Stelle lediglich ein

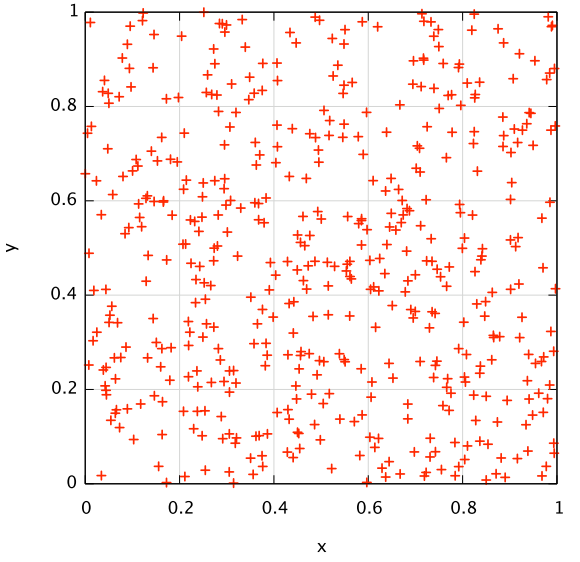

Abbildung 6.10 — Darstellung einer Sequenz von 1000 Zufallszahlen aus dem Intervall $(0, 1)$, die paarweise zusammengefaßt als (x, y)-Koordinaten von 500 Punkten interpretiert werden. Damit gelingt ein zwar naiver aber wirkungsvoller Test bezüglich der Qualität der Zufallszahlensequenz: Zeichnen sich in einem solchen Diagramm keine auffälligen periodischen Strukturen ab, so kann zunächst von einer guten Qualität der Zufallszahlen ausgegangen werden.

verblüffend einfaches Testverfahren. Dazu wird eine Sequenz von Zufallszahlen erzeugt. Diese werden nun paarweise gelesen, als (x, y)-Koordinaten interpretiert und in ein Diagramm eingetragen (⇝Abbildung 6.10).

Betrachtet man ein solches Diagramm, so bieten menschliches Auge und vor allem Mustererkennungen einen zwar naiven, aber sehr wirkungsvollen Test bezüglich der Qualität der Zufallszahlen. Zeichnen sich in einem solchen Diagramm keine auffällig periodischen Strukturen ab, kann eine gute Qualität der Zufallszahlen angenommen werden.

6.5 Software

Die verschiedenen Programme, die zur Verwirklichung der Destillation und Purifikation von Quantenzuständen verwendet werden, können in drei Grup-

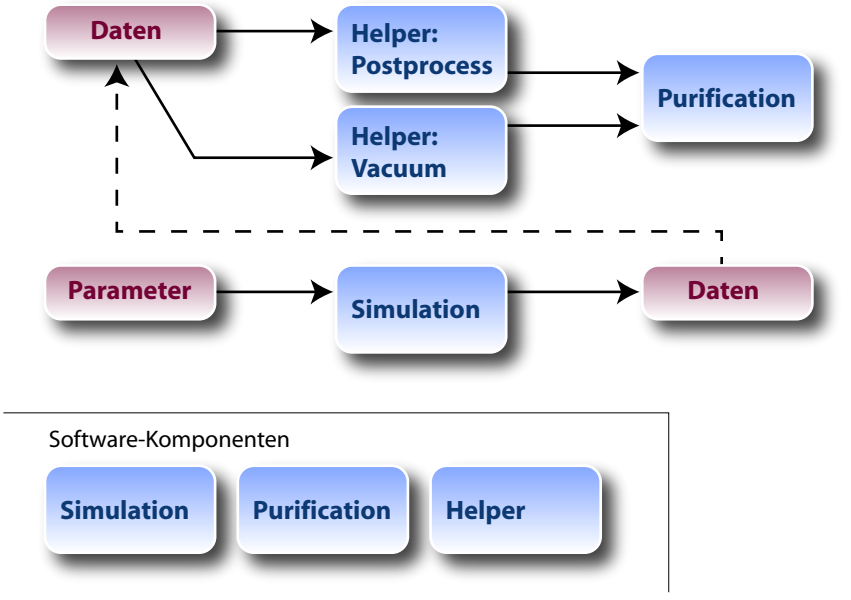

Abbildung 6.11 — Übersicht über die verwendeten Softwarekomponenten. Die einzelnen Programme und Routinen können einer der drei Gruppen *Simulation*, *Purifikation* und *Helper* zugeordet werden. Das Diagramm zeigt den prinzipellen Arbeitsablauf.

pen unterteilt werden (siehe auch ⇝Abbildung 6.11). Zum einen exisitieren Routinen, mit denen eine numerische Simulation durchgeführt werden kann („Simulation“). Das Programm produziert Ausgabedateien, die in Struktur und Inhalt gemessenen Daten entsprechen. Weiter gibt es Routinen, die zur Auswertung dienen („Purification“). Diese können simulierte wie auch gemessene Daten verarbeiten. Als dritte Gruppe gibt es eine Reihe von Hilfsroutinen für verschiedene Aufgaben („Helper“). Als wichtigste Routine dieser Gruppe ist ein Programm anzusehen, mit dem gemessene Daten nachbearbeitet werden können, um den Einfluß der nichtlinearen Phase des Antialias-Filters zu kompensieren. Die kompletten Quellcodes der verwendeten Software sind im ⇝Anhang (A) wiedergegeben. Ein großer Vorteil der Softwarenentwicklung in `Python` besteht durch die reduzierte Syntax darin, dass der Quellcode der Programme als Pseudocode gelesen werden kann und instruktiver ist als eine längliche Besprechung der Funktionen. Daher erfolgt an dieser Stelle die Beschränken auf eine Dokumentation der grundlegenden Funktionsweise.

6.5.1 Simulation

Ziel des Simulationsprogrammes ist es, Datenreihen zu erstellen, die die gleiche Struktur haben, wie solche, die durch reale Messungen gewonnen werden können. Ein anderer Ansatz beruht auf der Festellung, dass die Vorgänge bei der Purifikation von Quantenzuständen analytisch gut verstanden sind. Man könnte also auch eine Simulation betreiben, der eine Analytik zugrunde liegt und die im Lösen von Integralen besteht. Der hier verwirklichte Ansatz verzichtet auf diese Analytik und funktioniert rein numerisch. Zum Funktionsprinzip kann man ⇝Abbildung 6.12 betrachten. Die *simulierte Erzeugung von Messwerten* benötigt eine Reihe von Eingabeparametern:

1 | `opa1amp_value/opa1pha_value`. Die Varianzen der Amplituden- und Phasenquadraturen von OPA1 und OPA2. Dies sind lineare Varianzen bezogen auf ein Vakuumrauschen von 1. Ein Wert von 0,5 entspricht also einer Rauschunterdrückung von -3 dB. Die Möglichkeit, unabhängig voneinander Werte für gequetschte und antigequetschte Quadratur vorzugeben, ermöglicht es, auch gemischte Zustände (wie sie im Experiment auftreten) bearbeiten zu können.

2 | `outfilename`. Der Name der Ausgabedatei

3 | `sigma_of_noise`. Die Standardabweichung des Phasenrauschens

4 | `modus`. Ein Schalter, mit dem gesteuert werden kann, welche Quadraturwerte in die Ausgabedatei geschrieben werden.

5 | `number_of_points`. Länge der Ausgabedatei. Ein typischer Wert liegt zwischen 10^5 und 10^6.

Die Software erzeugt vier Zahlenreihen (*arrays*) die jeweils die Länge von `number_of_points` haben und mit Zufallszahlen gefüllt werden. Die Zufallszahlen weisen dabei eine gaußsche Verteilung auf und haben eine bekannte Varianz, die jeweils durch die vier Eingabeparameter `opaxYYY_value` gegeben sind, wobei `x` die OPAs numeriert und `YYY` $= \{$`AMP`, `PHA`$\}$ die Amplitudenquadratur oder die Phasenquadratur benennt.

Ebenso werden zwei *arrays* mit Phasenrauschwerten gefüllt. Das Phasenrauschen hat eine vorgegebene Standardabweichung und wird durch den Helper `MakeNoise` per DSP bandpassgefiltert.

Anschließend wird das Phasenrauschen auf die Messwerte angewendet. Auf diesem Weg wird die Transmission durch einen optischen Kanal repräsentiert.

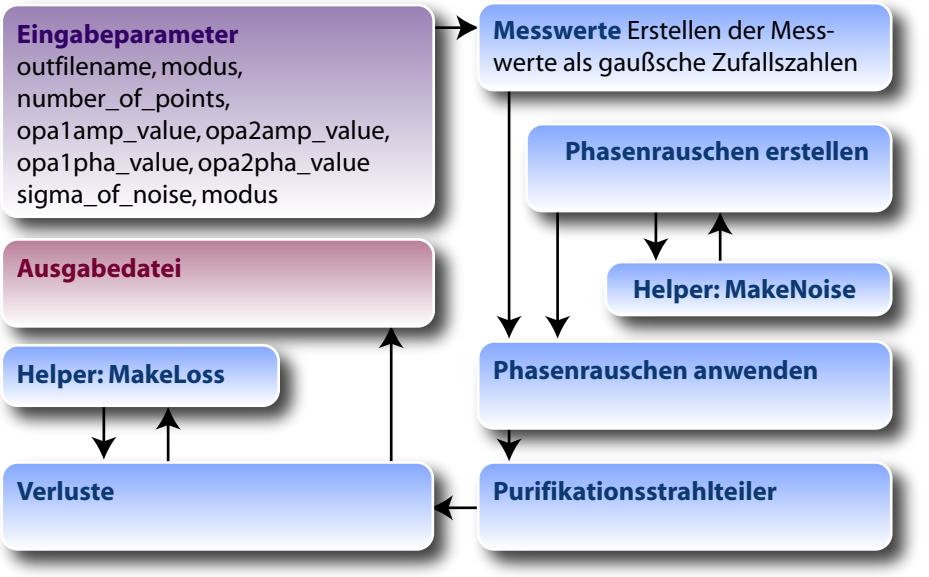

Abbildung 6.12 — Blockdiagramm der Simulationsroutine. Entsprechend der Eingabeparameter werden Messwerte generiert und mit zufälligem Phasenrauschen versehen. Nach der Auswertung der Strahlteilergleichung am Purifikationsstrahlteiler können zusätzlich Detektionsverluste eingefügt werden. Schließlich wird eine Ausgabedatei generiert, die in ihrem Inhalt experimentell gewonnenen Daten entspricht und weiter verarbeitet werden kann.

Als nächste Stufe wird die Wirkung des Purifikationsstrahlteilers simuliert. Dazu werden die beiden simulierten Zustände (jeweils bestehend aus einem *array*, welches die Amplitudenmesswerte und einem, welches die Phasenmesswerte enthält) gemäß der Strahlteilergleichung (⇝Anhang (B)) miteinander kombiniert. Man erhält vier neue *arrays*, die die Messwerte von jeweils Amplitude und Phase in den beiden Ausgängen des Strahlteilers beschreiben. Dies geschieht gemäß

$$\begin{aligned}
\text{port1amp[i]} &= (\text{opa1amp[i]} + \text{opa2amp[i]})2^{-1/2}, && (6.31)\\
\text{port1pha[i]} &= (\text{opa1pha[i]} + \text{opa2pha[i]})2^{-1/2}, && (6.32)\\
\text{port2amp[i]} &= (\text{opa1amp[i]} - \text{opa2amp[i]})2^{-1/2}, && (6.33)\\
\text{port2pha[i]} &= (\text{opa1pha[i]} - \text{opa2pha[i]})2^{-1/2}. && (6.34)
\end{aligned}$$

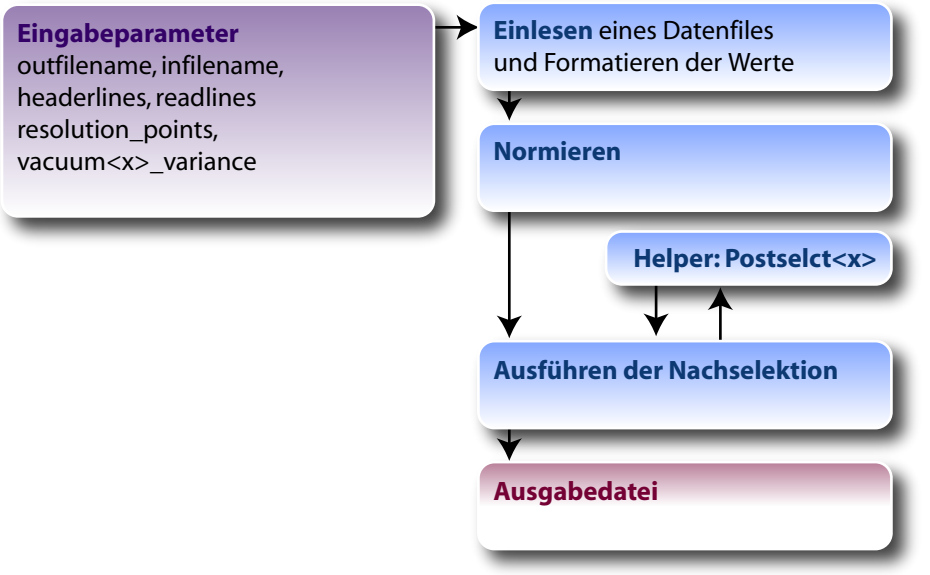

Abbildung 6.13 — Blockdiagramm der Destillationsroutine. Eine Datei wird eingelesen (Messdaten oder Simulation) und gegebenenfalls normiert (Vakuumrauschen = 1). Danach wird die Nachselektion mit der gewünschten Routine durchgeführt und eine Ausgabedatei erstellt.

Die beiden Ausgänge des Purifikationsstrahlteilers können nun vermessen werden. Dazu wird eine Ausgabedatei erstellt, in das – durch den Schalter `modus` festgelegt – nun eine beliebige Kombination aus Amplituden- und Phasenquadraturmesswerten geschrieben wird. An beliebiger Stelle im Laufe der Propagation der Messwerte kann zusätzlich der Helper `MakeLoss` eingeführt werden, der einen beliebigen optischen Verlust einfügt. Im Allgemeinen wird dieser Helper nicht verwendet, da die Eingabewerte der Quadraturmesswerte bereits Verluste beinhalten und es keine Rolle spielt, ob diese vor (Propagationsverluste) oder nach (Detektionseffizienz) dem Purifikationsstrahlteiler zum Tragen kommen.

6.5.2 Auswertung

Herzstück der vorliegenden Arbeit ist eine einfache Routine zur Nachselektion von real gemessenen oder durch Simulation gewonnen Datenreihen. Das Funktionsprinzip kann der ⇝Abbildung 6.13 entnommen werden. Die

Routine erwartet die Angabe einer Reihe von Eingabeparametern:

1 | `infilename` und `oufilename`. Namen von Eingabe und Ausgabefile.

2 | `headerlines` und `readlines`. Ermöglichen das Ignorieren von Header-Informationen im Eingabefile. Eine Anzahl `headerlines` von Zeilen zu Beginn der Datei werden ignoriert, anschließend eine Anzahl `readlines` eingelesen.

3 | `resolution_points`. Legt die Auflösung der Schwellenwerte fest, mit der die Ausgabedatei erzeugt werden soll.

4 | `vacuum1_variance` und `vacuum2_variance`. Bezeichnet die Vakuumreferenzen, auf die die Daten normiert werden sollen. Im Fall simulierter Daten ist die Normierung schon erfolgt, beide Werte werden dann auf 1 gesetzt. Im Fall gemessener Daten müssen die Referenzen durch den Helper `vacuum` zunächst berechnet und dann mit übergeben werden.

Es spielt für diese Routine keine Rolle, ob gemessene oder simulierte Daten vorliegen. Die Messdaten zweier Detektoren werden zunächst eingelesen und in geeigneter Weise formatiert (in *arrays* abgelegt). Details dazu kann man am besten einfach aus dem Quellcode herauslesen (⇝Anhang (A)). Anschließend werden die Datenreihen auf das (im Fall gemessener Daten zunächst festzustellende) Vakuumrauschen normiert. Die eigentliche Destillation und Purifikation entsteht durch paarweises Vergleichen von je zwei Messwerten mit gleichem Index aus den beiden *arrays*. Das Auswahlkriterium benötigt den aktuellen Schwellenwert und wird von einem Helper erledigt. Die Wahl des Helpers ermöglicht auch die Durchführung von *quantum channel probing* (Kapitel 7). Durch dieses modulare Konstruktionsprinzip kann die verwendete Software leicht erweitert werden. Zuletzt werden die erhaltenen Daten in eine Ausgabedatei abgelegt. Ein solches Ausgabefile enthält drei Spalten. Die erste Spalte enthält einen Wert für den Schwellenwert, die zweite Spalte enthält die Varianz des mit diesem Schwellenwert purifizierten Datenstroms, die dritte Spalte enthält die Erfolgswahrscheinlichkeit P, also das Verhältnis von der Länge des purifizierten Datenstroms zur Länge des Eingabedatenstroms.

6.5.3 Helper

In der Kategorie „Helper“ fassen wir eine Reihe kleiner Hilfsprogramme und Subroutinen zusammen. Die Bezeichnung Helper ist dabei eigentlich irreführend, da ein wesentlicher Teil der Arbeit von diesen Routinen erledigt wird.

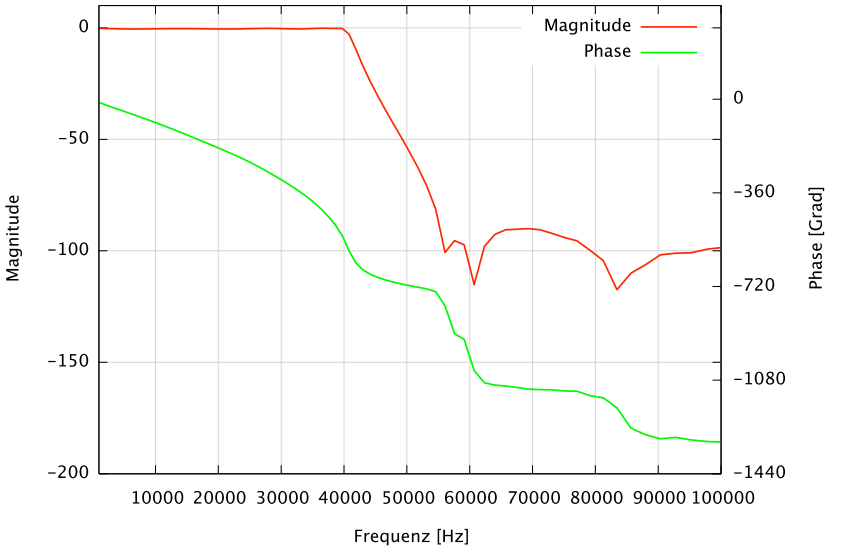

Abbildung 6.14 — Die Transferfunktion des Antialiasing-Filters (erster Kanal). Die Transferfunktion des zweiten Kanals verläuft identisch zu dieser.

1 | **Postprocess** Diese Routine stellt (zusammen mit `PostselectX`) vermutlich den wesentlichsten Teil der Software dar. Die Routine bereinigt die Effekte des nichtlinearen Phasenganges, der vom Antialiasing-Filter eingeführt wird. Die ⇝Abbildung 6.14 zeigt die gemessene Transferfunktion des ersten Kanals dieses Filters (die Transferfunktion des zweiten Kanals ist praktisch identisch – sie wird hier nicht gezeigt, wohl aber für die Berechnungen benutzt). Funktionsprinzip: Der Inhalt eines Datenfiles (zwei Spalten von Meßwerten) wird geladen und per FFT transfomiert. Dies liefert komplexe Werte. Die gemessene Phase der Transferfunktion wird importiert und formatiert. Für jede Frequenz des Spektrums der FFT wird der tatsächliche Phasenwert aus der Transferfunktion durch lineare Interpolation gewonnen und mit der entsprechenden Fourierkomponente multipliziert:

```
fft[i] = fft[i] * exp(-1j * phasethere[0] * 2.0 * pi /360.0)
```

Anschliessend wird die inverse FFT von `Python` bemüht, um wieder eine Zeitserie zu erhalten.

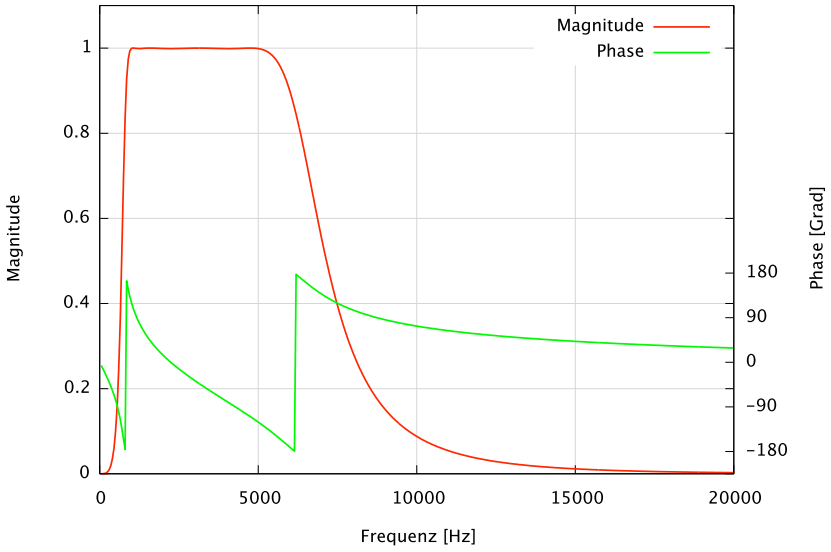

Abbildung 6.15 — Die Transferfunktion des Phasenrauschfilters. Der Filter ist als digitaler Chebychev-Bandpass realisiert. Die zugehörigen Filterkoefizienten lauten:

$a_0 = 0{,}00045921618388999088$ $b_0 = 1{,}0$
$a_1 = 0{,}0$ $b_1 = -7{,}1732007945$
$a_2 = -0{,}0018368647355599635$ $b_2 = 22{,}6385602238$
$a_3 = 0{,}0$ $b_3 = -41{,}0695071546$
$a_4 = 0{,}0027552971033399454$ $b_4 = 46{,}8533814786$
$a_5 = 0{,}0$ $b_5 = -34{,}4255969981$
$a_6 = -0{,}0018368647355599635$ $b_6 = 15{,}9105081693$
$a_7 = 0{,}0$ $b_7 = -4{,}2291670230$
$a_8 = 0{,}00045921618388999088$ $b_8 = 0{,}4950222052$

Der Filter ist, wie man sieht, als IIR-Filter ausgeführt und dient dem Zweck, das aufgebrachte Phasenrauschen auf ein Frequenzband zwischen 1 kHz und 5 kHz einzuschränken.

2 | **Powerspectrum** Diese Routine ermöglicht es, ein einfaches Leistungsspektrum eines Datenstroms darzustellen. Hierzu wird die FFT-Funktion von `Python` implementiert:

```
pwrspec = abs(vals_fft * conjugate(vals_fft))/len(vals)**2
```

3 | **Vacuum** Bei dieser Routine handelt es sich um ein einfaches Programm, welches die beiden Varianzen der Spalten eines Standard-Eingabefiles berechnet und ausgibt. Die Bezeichnung resultiert aus der ursprünglichen Anwendung: Normierungsfaktoren für Meßdaten zu liefern, die

eine Normierung auf das Vakuumrauschen ermöglichen. Funktionsprinzip: Einlesen eines Datenfiles → Formatieren der Werte → Subtraktion eines konstanten Offsets → Berechnung der Varianz als gewichtete Summe der quadratischen Abweichungen.

4 | **PostselectX** Die Routinen PostSelect1, Postselect2 und PostSelect4 stellen in gewissem Sinne das Herzstück des Destillationsalgorithmus dar. Bei den Routinen handelt es sich um einen einfachen Koinzidenzwähler. Er erhält als Eingabe zwei *arrays* von Messwerten (entsprechend den beiden Ausgängen des Purifikationsstrahlteilers) und einen Schwellenwert. Die Routinen konstruieren ein neues *array*, in das alle Werte des ersten *arrays* einsortiert werden, *falls* der korrespondierende Wert des zweiten *arrays* kleiner ist, als der vorgegebene Schwellwert. Die Routinen Postselect2, Postselect3 usw. werden zum *quantum channel probing* benötigt. Sie lassen einen Wert passieren, falls *X aufeinander folgende* Werte aus dem ersten Array kleiner als der Schwellwert sind.

5 | **MakeNoise** Diese Routine erstellt und bearbeitet das Phasenrauschen. Zunächst wird das Phasenrauschen in Form eines *arrays* mit gaußschen Zufallszahlen erstellt, welche eine vorgegebene Standardabweichung aufweisen. Im Experiment ist das Phasenrauschen jedoch auf ein relativ schmales Band zwischen 1 kHz und 5 kHz beschränkt. Dies wird auf Seiten der Simulation dadurch bewerkstelligt, dass die Zeitserie der Phasenrauschwerte mit einem digitalen Chebychev-Filter bearbeitet werden, was durch die Funktion MakeNoise umgesetzt wird. Die Transferfunktion dieses Filters ist zusammen mit den entsprechenden Filterkoeffizienten in ⇝Abbildung 6.15 wiedergegeben.

6 | **MakeLoss** Die Routine MakeLoss simuliert einen optischen Verlustkanal. Dieser wird durch einen Strahlteiler mit einem offenen Eingang realisiert. Der Strahlteiler hat eine variable Reflektivität, die die Stärke des Verlustes bestimmt. Durch den offenen Eingang des Strahlteilers koppelt Vakuumrauschen ein. Dieses Vakuumrauschen wird durch eine Sequenz gaußverteilter Zufallszahlen mit Varianz $V_{\text{vac}} = 1$ repräsentiert.

KAPITEL 7

Ergebnisse

In diesem Kapitel werden experimentell gewonnene Ergebnisse präsentiert und im Vergleich mit numerischen Simulationen diskutiert. Wie sich zeigen wird, weist das in Kapitel 4 entwickelte Destillationsprotokoll weit mehr Möglichkeiten auf, als eine zunächst naive Betrachtung vermuten läßt. Insbesondere die Erweiterungen des Protokolls aus Kapitel 4 mittels *conjugate purification* (CP) und die Möglichkeit des *quantum channel probing* (QCP) wurden im Rahmen dieser Arbeit zunächst als rein experimentelle Befunde entdeckt. Eine genauere Betrachtung und Vervollständigung der Theorie *folgte* der experimentellen Beobachtung.

Als Konvention legen wir fest, dass generell für alle Graphen dieses Kapitels gilt, dass durchgezogene Linien Daten repräsentieren, die mittels numerischer Simulation (Kapitel 6) gewonnen wurden, wohingegen Punkte experimentell gewonnene Messwerte repräsentieren.

Alle hier dargestellten Ergebnisse konnten an dem in Kapitel 5 detailliert beschriebenen experimentellen Aufbau gewonnen werden. Zwischen verschiedenen Experimenten waren lediglich kleinere Modifikationen der Elektronik notwendig. Man erinnere sich an die dreistufige Gliederung des Experimentes in *Generierung der Zustände*, *Transmission* und *Purifikation/Detektion*. Als vierter Grundbaustein ist die Datenbearbeitung und -analyse teilweise Bestandteil des Protokolls. Für die hier dargestellten Ergebnisse wurden zwei Kopien eines Zustandes präpariert, die beide Varianzen $V_x = 0{,}32$ und $V_p = 8{,}6$ aufwiesen. Diese Zustände wurden mit unabhängigem Phasenrauschen kontrollierbarer Stärke versehen, um den Effekt einer Übertragung durch einen optischen Kanal nachzubilden und anschließend phasenstarr auf einem Strahlteiler überlagert. Die beiden Ausgänge des Strahlteilers wurden mit je einem

Homodyndetektor vermessen, wobei einer der Detektoren ein Triggersignal generiert und der andere Detektor lediglich der Verifikation dient und – im Prinzip – durch ein beliebiges quantenoptisches Experiment ersetzt werden kann, das vom durchgeführten Destillationsprotokoll profitieren soll.

7.1 Einfache Purifikation

Als „einfache Purifikation“ bezeichnen wir das in Kapitel 4 entwickelte Protokoll, bei dem ein Homodyndetektor in einem Ausgang des Purifikationsstrahlteilers die ursprünglich gequetschte Quadratur x_1 misst. Wird dabei gefunden, dass der erhaltene Meßwert betragsmäßig kleiner ist als ein fest gewählter Schwellenwert Q, so wird der zeitgleich im anderen Ausgang des Purifikationsstrahlteilers vorliegende Meßwert der dortigen Quadratur x_2 „akzeptiert“, andernfalls „abgelehnt“. In ⇝Abbildung 7.1 wurden die beiden Kopien des gequetschten Zustandes mit einem Phasenrauschen fester Stärke versehen und mittels Konditionierung $|x_1| < Q$ mit dem Destillationsprotokoll bearbeitet. Man erkennt zunächst, wie mit kleiner werdendem Schwellenwert Q die Varianz des Ausgabezustandes abnimmt. Genau dies ist der gewünschte Effekt einer Destillation des Quetschgrades. Man sieht jedoch auch, wie die gemessene Destillation des Quetschgrades hinter den theoretischen Erwartungen zurück bleibt. Um diese Abweichung zu verstehen, müssen wir die Effekte einer Signalfilterung erneut betrachten.

In Kapitel 6 hatten wir für ein Filter die Transferfunktion $H(s)$ definiert, die zwischen einem Filtereingabesignal $X(s)$ und dem Ausgabesignal $Y(s)$ vermittelt:

$$Y(s) = H(s)X(s). \tag{7.1}$$

Die Größen $X(s)$, $Y(s)$ und $H(s)$ sind dabei die Laplace-Transformierten von Zeitserien $x(t)$, $y(t)$ und $h(t)$. Insbesondere ist

$$H(s) = \int_{-\infty}^{\infty} h(t) \exp(-st) dt. \tag{7.2}$$

Die Funktion $h(t)$ ist die *Impulsantwort* des Systems. Wird ein solches System durch eine sinusförmige Anregung

$$x(t) = A(t) \cos(\omega t + \theta) \tag{7.3}$$

getrieben, so kann die Ausgabefunktion näherungsweise durch

$$y(t) = A(t - \tau_g) \cos(\omega(t - \tau_\phi) + \theta) \tag{7.4}$$

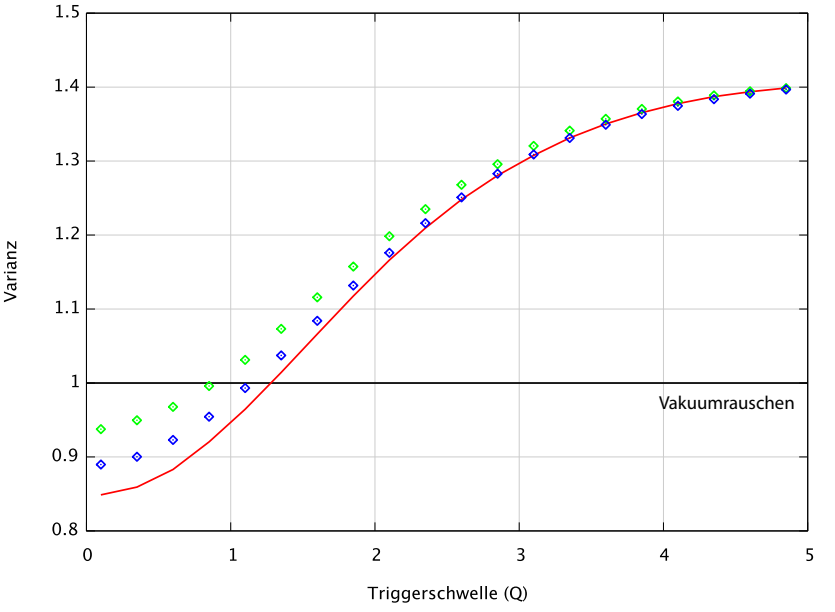

Abbildung 7.1 — Der Effekt der Nachbearbeitung der Daten. Die rote, durchgezogene Kurve zeigt eine Simulation für die Eingabeparameter $V_x = 0{,}32$ und $V_p = 8{,}6$. Die Stärke des Phasenrauschens betrug $\sigma = 0{,}392$. Prozessiert man Messdaten mit den entsprechenden Parametern, erhält man die in grün dargestellten Punkte, die Stärke der Destillation bleibt also hinter den Erwartungen zurück. Werden die Daten dagegen vor Anwendung des Destillationsprotokolls mit der Routine `postprocess` bearbeitet, erhält man die blaue Kurve, die der Simulation wesentlich besser entspricht.

dargestellt werden. Die Parameter τ_g und τ_ϕ heißen *Gruppenverzögerung* und *Phasenverzögerung* des Systems und können im Allgemeinen Funktionen von ω sein. Wir betrachten nun ein System mit einem linearen Phasengang, das heißt, $\theta(\omega)$ ist eine lineare Funktion der Frequenz. In diesem Fall kann man zeigen, dass τ_g und τ_ϕ gleich und konstant sind. Wird ein solches System von einer Eingabefunktion

$$x(t) = \exp(i\omega t) \tag{7.5}$$

getrieben, so lautet die Ausgabe

$$y(t) = |H(i\omega)| \exp(i(\omega t + \phi(\omega))), \tag{7.6}$$

wobei die Phasenverschiebung ϕ durch

$$\phi(\omega) = \arg(H(i\omega)) \tag{7.7}$$

definiert ist. Gruppen- und Phasenverzögerung hängen mit ϕ durch

$$\tau_g = -\frac{d\phi(\omega)}{d\omega} \tag{7.8}$$

und

$$\tau_\phi = -\frac{\phi(\omega)}{\omega} \tag{7.9}$$

zusammen. Von besonderer Bedeutung für das vorliegende Experiment ist dabei die Gruppenverzögerung. Ist diese nicht konstant, so kommt es zu einer zeitlichen Verbreiterung von Signalen. Eine konstante Gruppenverzögerung (*constant group delay*) kann erreicht werden, wenn die Transferfunktion des Gesamtsystems eine in der Frequenz lineare Phasenverschiebung aufweist. Betrachtet man aber zum Beispiel die Transferfunktion des im Experiment verwendeten Antialias-Filters (⇝Abbildung 6.14), so wird sofort klar, dass dies nicht der Fall ist. Glücklicherweise kann der Effekt dieses Filters rückgängig gemacht werden, was die Nachbearbeitungsroutine `postprocess` erledigt. Dazu werden die Zeitserien von Quadraturmeßwerten einer Fouriertransformation unterzogen. Die erhaltenen Frequenzkomponenten können nun mit der inversen Phase des Anti-Aliasing-Filters bei der entsprechenden Frequenz multipliziert werden. Durch inverse Fouriertransformation erhält man aus den derart bearbeiteten Frequenzkomponenten eine Zeitserie zurück.

Wird diese nachbearbeitete Zeitserie nun dem Destillationsprotokoll unterzogen, erhält man eine deutlich verbesserte Stimmigkeit mit den Vorhersagen (⇝Abbildung 7.1). Eine *perfekte* Übereinstimmung kann nicht erzielt werden, was auf weitere Filterungsprozesse im System zurückzuführen ist, die einen nichtlinearen Phasengang einführen. Es ist allerdings nicht ohne Weiteres möglich, eine Transferfunktion des Phasenganges des Gesamtsystems zu erhalten. Vor dem Hintergrund einer technologischen Implementierung des hier vorgestellten Destillationsverfahrens muss dieser Effekt (und damit die Notwendigkeit einer konstanten Gruppenverzögerung) unbedingt bedacht werden. Es wurde jedoch auch demonstriert, dass die nachteiligen Effekte (bei bekannter Transferfunktion) auch im Nachhinein beseitigt werden können.

In ⇝Abbildung 7.2 wird der Effekt einer Korrelation zwischen den beiden Rauschsignalen, mit denen die beiden Kopien des gequetschten Zustandes versehen werden, untersucht. Die rote Kurve ist dabei identisch mit der vorher gezeigten Kurve für eine feste Phasenrauschstärke $\sigma = 0{,}392$. Führt man nun eine Korrelation ein, die im Grenzfall darin übergeht, dass beide Rauschsignale identisch sind (grüne Kurve), so findet man, dass die Effektivität des

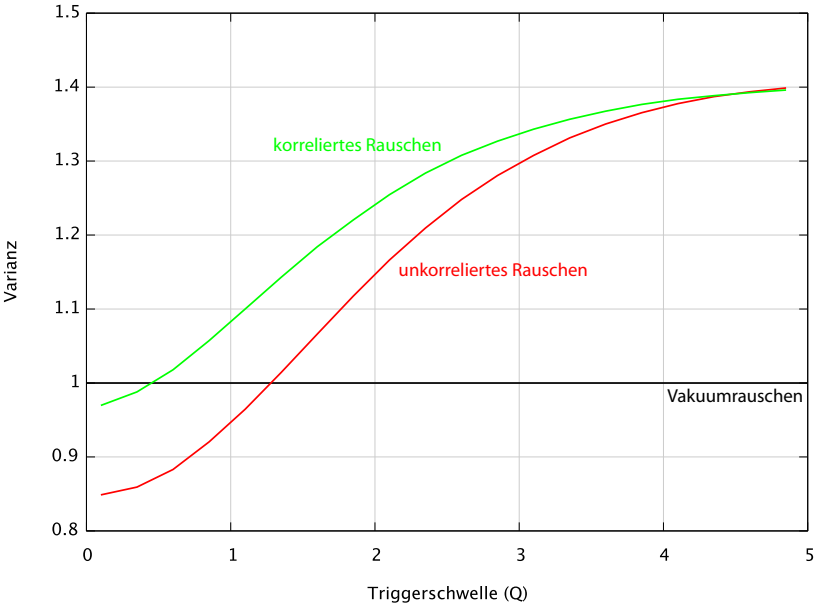

Abbildung 7.2 — Einfluss einer Korrelation zwischen den beiden Rauschsignalen, die die Kopien eines gequetschten Zustandes beeinträchtigen, auf die Destillation. Die rote Kurve ist identisch mit der entsprechenden Kurve aus der ⇝Abbildung 7.1. Die grüne Kurve ergibt sich, wenn die beiden Kopien eines gequetschten Zustandes durch vollständig korreliertes (nämlich identisches) Rauschen beeinträchtigt werden. Die Destillation des Quetschgrades ist dann weniger effektiv. Wenn man antikorreliertes Rauschen verwendet, ergibt sich ein Kurvenverlauf, der deckungsgleich zu der grünen Kurve ist.

Destillationsprotokolls erheblich verringert wird. Im Fall perfekter Antikorrelation erhält man dieselbe grüne Kurve. Diese Tatsache muß wiederum vor dem Hintergrund einer technologischen Implemetierung gewertet werden. Überträgt man die Kopien etwa zeitgleich über dasselbe Glasfaserkabel, so wird sich zwingend ein gewisses Maß an Korrelation einstellen, die eine Destillation des Squeezinggrades behindert. Einfacher als eine Übertragung über unterschiedliche Fasern ist dann eine Übertragung mit einer gewissen Zeitverzögerung, die durch hilfsweise aufgebrachte Zeitmarker definiert und identifiziert werden kann.

In ⇝Abbildung 7.3 wird exemplarisch die Wirkungsweise des Destillationsprotokolls für drei unterschiedliche Rauschstärken σ gezeigt. Man erkennt, wie für zunehmendes Phasenrauschen das Protokoll zunehmend effektiver

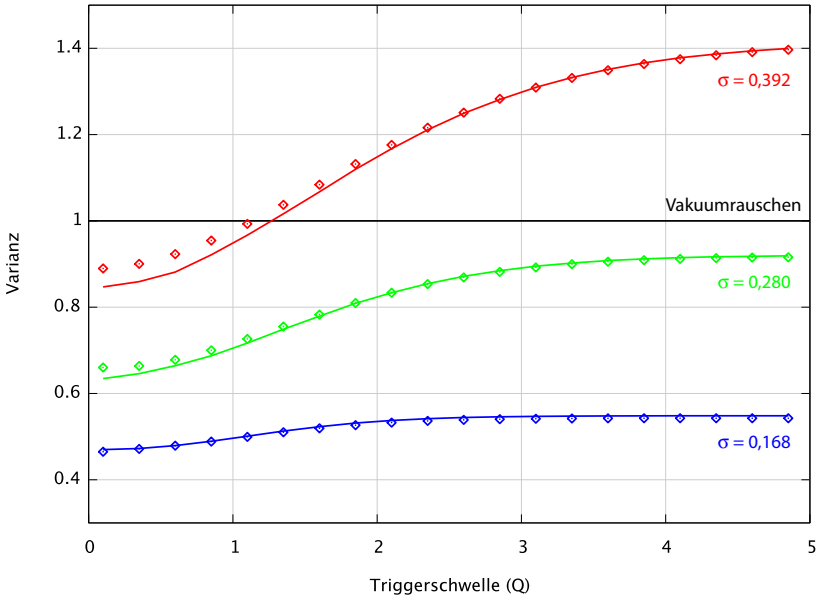

Abbildung 7.3 — Varianzen der Ausgabezustände nach der Destillation für drei unterschiedliche Werte des Phasenrauschens, nämlich $\sigma = 0{,}392$ (rot), $\sigma = 0{,}280$ (grün) und $\sigma = 0{,}168$ (blau). Durchgezogene Kurven zeigen die Simulation, während Messdaten durch Punkte illustriert sind. Mit kleiner werdendem Schwellenwert Q verkleinert sich monoton die Varianz des Zustandes nach der Destillation. Die Effektivität der Destillation nimmt mit größer werdendem Phasenrauschen zu. Man beachte, dass die rote Kurve unter der Destillation das Vakuumrauschen unterschreitet! Ein Zustand ohne nichtklassische Signatur wird durch das Destillationsprotokoll bemerkenswerterweise in einen nichtklassischen Zustand überführt.

wird (gemessen an der rückgewinnbaren Rauschunterdrückung). Bedenkt man den ursprünglichen Quetschgrad von $V_x = 0{,}32$, so wird auch klar, dass dieser ursprüngliche Quetschgrad in einem einzelnen Schritt nicht zurückgewonnen werden kann. Besondere Bedeutung kommt in dieser Abbildung der Kurve zu, die das Vakuumrauschen bei $V = 1$ schneidet: Während die beiden Kopien *vor* der Destillation durch die Wirkung des Phasenrauschens keine gequetschten Zustände mehr sind ($V > 1$), kann allein durch Anwendung des Destillationsprotokolls das Vakuumrauschniveau unterschritten werden. Man erhält aus zwei Zuständen *ohne* nichtklassische Signatur einen einzelnen Zustand zurück, dessen Varianz *unterhalb* der klassischen Grenze liegt!

Eine aussagekräftigere Darstellung erhält man, wenn man die Varianz des

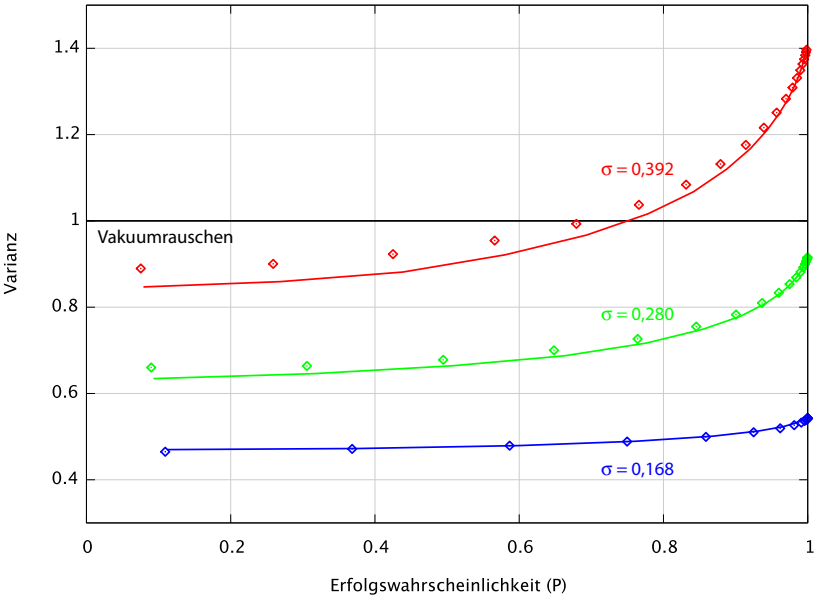

Abbildung 7.4 — Darstellung derselben Daten wie aus ⇝Abbildung 7.3, diesmal aufgetragen über der Erfolgswahrscheinlichkeit $\mathcal{P}$. Man erkennt, dass für Erfolgswahrscheinlichkeiten von einigen 10 Prozent bereits eine fast maximale Verringerung der Varianz stattgefunden hat. Eine weitere Verkleinerung der Erfolgswahrscheinlichkeit (entsprechend einer kleineren Wahl des Schwellenwertes Q) bringt nur noch eine geringfügige Verbesserung.

verbleibenden Zustandes nach der Destillation nicht über dem Schwellenwert Q, sondern über der *Erfolgswahrscheinlichkeit* $\mathcal{P}$ aufträgt ⇝Abbildung 7.4. In jeder technologischen Realisierung eines Quanteninformationsprotokolls kommt immer der erzielbaren Bandbreite eine hohe Bedeutung zu. Es ist also sinnvoller, nicht einen Schwellenwert vorzugeben, sondern vielmehr die Anzahl der Meßwerte zu benennen, die unter Wirkung des Protokolls (maximal) zurückgewiesen werden dürfen. Die Abbildung zeigt, dass bei einer vorgegebenen Erfolgswahrscheinlichkeit von zum Beispiel 0,5 bereits eine erhebliche Destillation des Squeezinggrades stattgefunden hat. Der Zusammenhang zwischen Schwellenwert Q und Erfolgswahrscheinlichkeit $\mathcal{P}$ kann in ⇝Abbildung 7.5 betrachtet werden. Dieser Zusammenhang variiert mit der Stärke des aufgebrachten Phasenrauschens. Wir nehmen jedoch an, dass in einem realistischen Szenario die Stärke des Phasenrauschens ein Charakteristikum des verwendeten Kanals – und insbesondere konstant – ist. In diesem

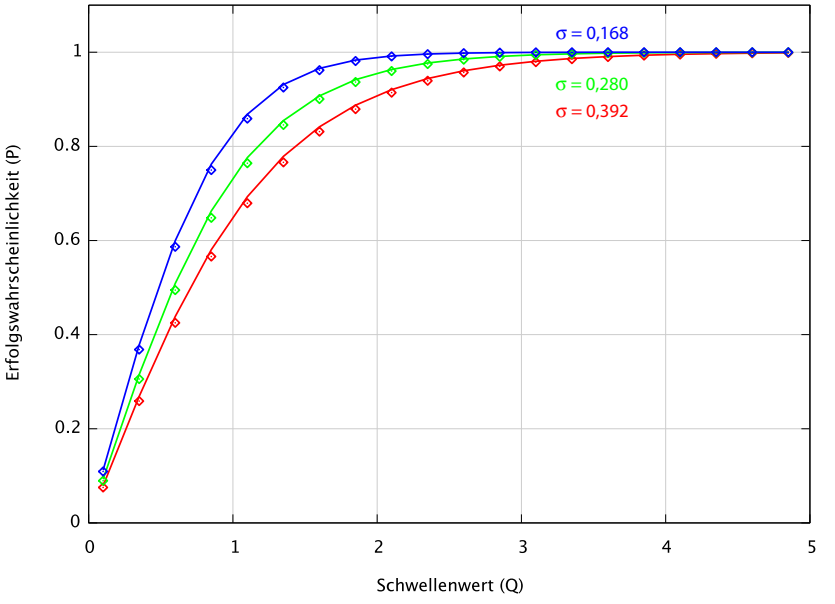

Abbildung 7.5 — Erneute Darstellung der Daten aus Abbildung ⇝Abbildung 7.3. Diesmal in einer Darstellung, in der die Erfolgswahrscheinlichkeit $\mathcal{P}$ über dem Schwellenwert Q aufgetragen ist. Die Form der Kurven folgt etwa der erf()-Funktion. Entscheidend ist die Existenz eines eindeutigen und monotonen Zusammenhangs zwischen $\mathcal{P}$ und Q (siehe Text). Der genau Verlauf der Kurve hängt von der Stärke des vorhandenen Phasenrauschens ab. (Farbzuordnung wie in ⇝Abbildung 7.3).

Fall bekannten Phasenrauschens kann aus einer zu ⇝Abbildung 7.5 vergleichbaren Abbildung ein eindeutiger Zusammenhang zwischen Schwellenwert Q und Erfolgswahrscheinlichkeit P abgeleitet werden, der als Eichung dient.

Die ⇝Abbildung 7.6 kann als Zusammenfassung der Ergebnisse dieses Abschnitts gelesen werden. Dargestellt ist wieder die Wirkung des Destillationsprokolls, diesmal aufgetragen über der Stärke des Phasenrauschens. Die obere Kurve zeigt die Varianz des Eingangszustandes vor der Destillation, die rote Kurve zeigt die Varianz nachdem mit einem Schwellenwert von 1 destilliert wurde (entsprechend Erfolgswahrscheinlichkeiten zwischen etwa $P = 0{,}5$ und $P = 0{,}9$). Ein interessantes Regime findet man im Bereich $0{,}3 < \sigma < 0{,}41$, in dem die Kopien eines gequetschten Zustandes vor Anwendung des Destillationsprotokolls keine nichtklassischen Eigenschaften mehr aufweisen, die verbleibende Kopie *nach* Anwendung des Destillationsprotokolls jedoch wie-

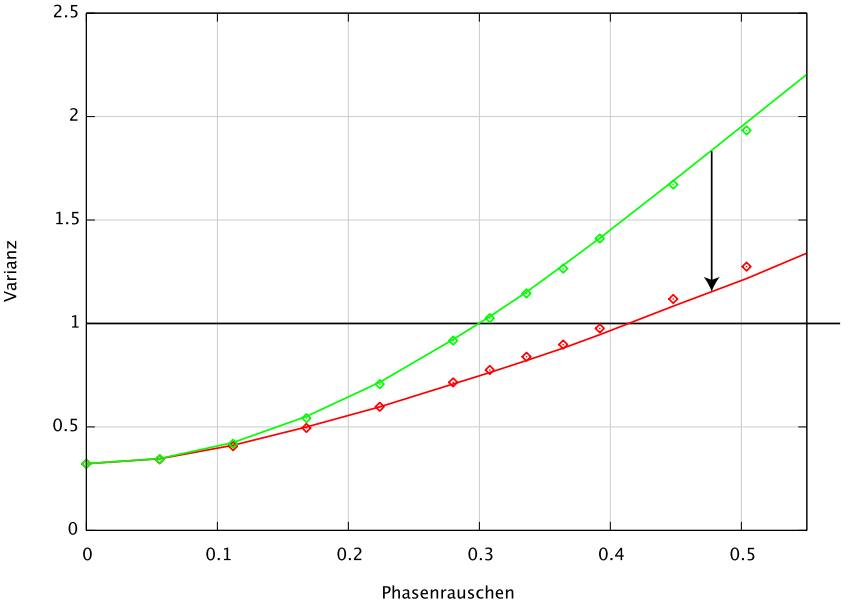

Abbildung 7.6 — Demonstration des Destillationsprotokolls für verschiedene Stärken des Phasenrauschens. Die Kurven zeigen die Varianz der ehemals gequetschten Quadratur vor (grün) und nach (rot) der Destillation. Die rote Kurve erhält man, wenn man als Schwellenwert $Q = 1$ ansetzt.

der ein gequetschter Zustand ist, der nichtklassische Eigenschaften aufweist und zur Durchführung von Quantenprotokollen genutzt werden kann.

7.2 Conjugate Purification

Wir hatten im vorhergehenden Abschnittt gezeigt, wie durch eine Konditionierung $|x_1| < Q$ eine Destillation des Squeezinggrades gelingt, wie also aus zwei phasenverrauschten Zuständen mit geringer (oder keiner!) nichtklassischer Rauschunterdrückung ein einzelner Zustand größerer Rauschunterdrückung gewonnen werden kann. Erstaunlicherweise findet man (⇝Abbildung 7.7), dass eine Destillation auch dann stattfindet, wenn man statt auf der ursprünglich gequetschten auf der ursprünglich *antigequetschten* Quadratur konditioniert, also ein Kriterium der Form $|p_1| < Q$ anwendet. Da also zur Konditionierung die zur beobachteten Quadratur konjugierte Quadratur her-

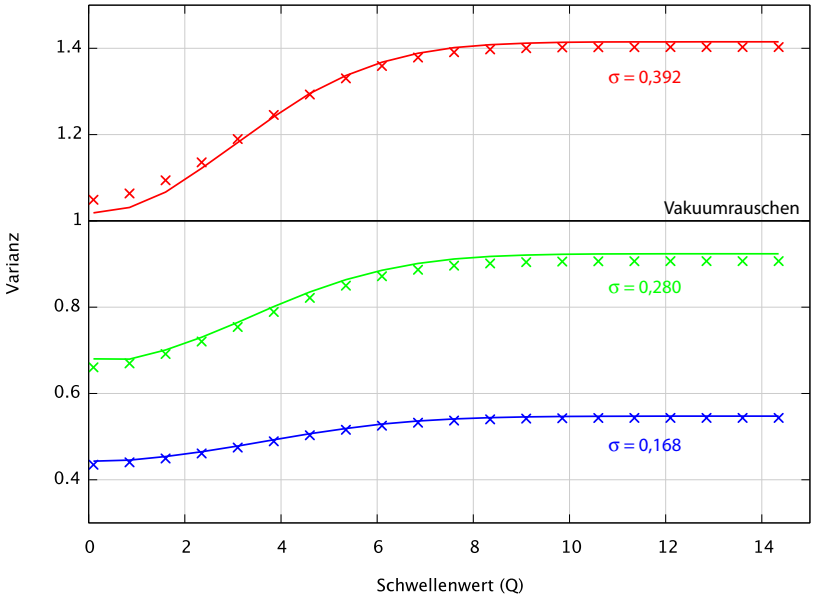

Abbildung 7.7 — Ausgabevarianzen V_{out}, bei einer Konditionierung auf der antigequetschten Quadratur $|p_1| < Q$ (*conjugate purification*) für drei unterschiedliche Stärken des Phasenrauschens, nämlich wie schon zuvor $\sigma = 0{,}392$ (rot), $\sigma = 0{,}280$ (grün) und $\sigma = 0{,}168$ (blau).

angezogen wird, bezeichnen wir diese Strategie als *conjugate purification* (CP).

Bemerkenswerterweise erhöht eine Konditionierung auf der antiquetschten Quadratur $|p_1| < Q$ nicht nur das Squeezing, sondern ist im Regime hinreichend kleinen Phasenrauschens sogar *effektiver* als die zuvor beschriebene Konditionierung $|x_1| < Q$. Diese Tatsache ist überraschend, da man naiv annehmen würde, dass eine Konditionierung auf $|p_1| < Q$ zwar die Varianz von p_2 reduzieren würde aber gleichzeitig eine Vergrößerung der Varianz von x_1 bewirkt. Man würde nämlich argumentieren, dass *kleine* Werte von p_1 genau dann wahrscheinlich sind, wenn die momentanen Phasenverschiebungen ϕ_1 und ϕ_2 von solcher Größe sind, dass die Zustände, die auf den Purifikationsstrahlteiler treffen, gerade in der p-Quadratur gequetscht sind. Diese klassische Vorstellung ist jedoch zu grob vereinfacht und spiegelt die tatsächlichen Verhältnisse nicht hinreichend wieder.

Um die Vorgänge zu verstehen, die *conjugate purification* ermöglichen, greifen wir die Berechnungen aus Kapitel 4 erneut auf. Dort hatten wir die Ausga-

bevarianzen für eine Konditionionierung auf der x_1-Quadratur berechnet. Wir führen nun die Rechnung analog, wobei wir eine Konditionierung auf einer *beliebigen* Quadratur $q_1 = x_1 \cos(\theta) + p_1 \sin(\theta)$ zulassen. Diese Quadratur wird von einem Homodyndetektor vermessen und ein positives Konditionierungssignal generiert, falls $|q_1| < Q$. Wir gehen wieder davon aus, dass vor der Anwendung des Phasenrauschens beide Kopien in der x-Quadratur gequetscht sind.

Wir können dann analog zu Kapitel 4 die Verbundwahrscheinlichkeit $P(q_1, x_2)$ angeben, die die Wahrscheinlichkeit bezeichnet, im einen Ausgang des Purifikationsstrahlteilers den Wert q_1 und zeitgleich im anderen Ausgang den Wert x_2 zu messen. Diese lautet (vergleiche auch [Hag07])

$$P(q_1, x_2) = \frac{1}{2\pi D} \exp\left[-\frac{Bq_1^2 + Ax_2^2 - 2Cq_1x_2}{2D}\right]. \tag{7.10}$$

Hierbei bezeichnen A und B die Varianzen der Quadraturen q_1 und x_2, bewertet für den Zustand im Ausgang des Purifikationsstrahlteilers:

$$\begin{aligned} A &= \frac{V_{x1} + V_{x2}}{2} \cos^2(\theta) + \frac{V_{p1} + V_{p2}}{2} \sin^2(\theta) \qquad (7.11)\\ &+ \frac{V_p - V_x}{4} [\sin(2\phi_1) + \sin(2\phi_2)] \sin(2\theta), \\ B &= \frac{V_{x1} + V_{x2}}{2}. \qquad (7.12) \end{aligned}$$

C bezeichnet die Korrelation zwischen den Quadraturen q_1 und x_2 und D ist zur Abkürzung gesetzt:

$$\begin{aligned} C &= \frac{V_{x1} - V_{x2}}{2} \cos(\theta) + \frac{V_p - V_x}{4} [\sin(2\phi_1) - \sin(2\phi_2)] \sin(\theta), \qquad (7.13)\\ D &= AB - C^2. \qquad (7.14) \end{aligned}$$

Davon ausgehend berechnet man wie im Kapitel 4 die Ausgabevarianz:

$$V_{\text{out}} = \frac{1}{\mathcal{P}} \int_{\phi_1} \int_{\phi_2} \left[B\,\text{erf}\left(\frac{Q}{\sqrt{2A}}\right) - \sqrt{\frac{2}{\pi}} \frac{C^2 Q}{A^{3/2}} e^{-Q^2/2A} \right] \Phi(\phi_1)\Phi(\phi_2) d\phi_1 d\phi_2. \tag{7.15}$$

Um zu verstehen, warum eine Konditionierung auf der antigequetschten Quadratur eine Destillation des Quetschgrades erzielt, betrachten wir ⇝Gleichung (7.15). Dort findet man im Wesentlichen zwei Terme. Im ersten Term (proportional B) wird der Faktor $\text{erf}(Q/\sqrt{2A})$ für verschwindendes

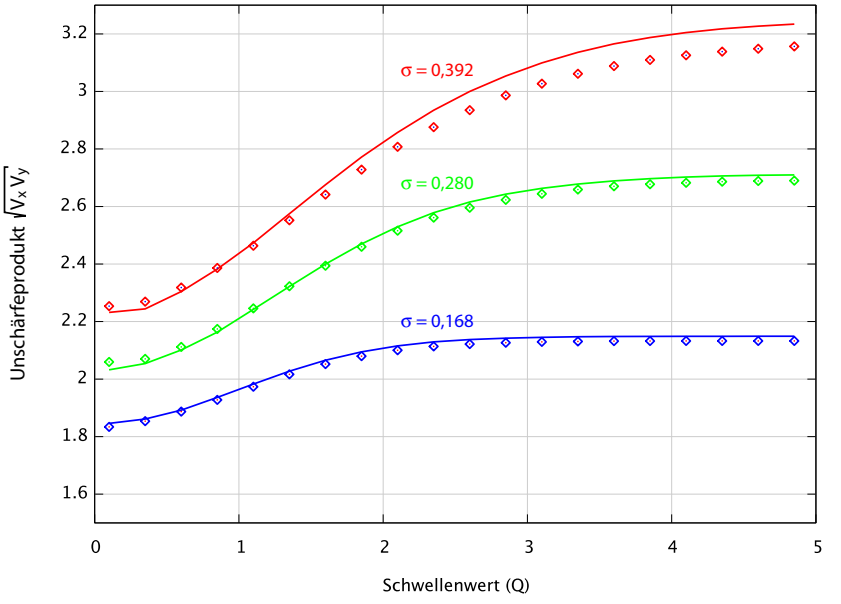

Abbildung 7.8 — Darstellung des Unschärfeproduktes $U = \sqrt{V_x V_p}$ über dem Schwellenwert Q für drei unterschiedliche Stärken des Phasenrauschens ($\sigma = 0{,}392$ (rot), $\sigma = 0{,}28$ (grün) und $\sigma = 0{,}168$ (blau)). Für einen gaußschen Zustand definiert man die Reinheit als $P = 1/U$. Da die Zustände für kleines Phasenrauschen gaußähnlich sind, ist die Abnahme des Unschärfeproduktes ein starker Beleg für eine Zunahme der Reinheit unter dem Destillationsprotokoll.

Phasenrauschen maximiert, wenn man auf x_1 konditioniert. In diesem Fall nimmt B seinen Minimalwert $B = V_x$ an. Dann wirkt die Konditionierung wie ein Filter, das Ereignisse, die mit einer großen Phasenverschiebung einhergehen, ausblendet. Die ⇝Gleichung (7.15) enthält jedoch noch einen zweiten, negativen Term, proportional zu C^2Q, der stets eine Verkleinerung der Varianz V_{out} bewirkt. Dieser zweite Term beschreibt einen reinen Quanteneffekt, denn er entsteht durch die Quanteninterferenz bei der Überlagerung der beiden Kopien eines phasenverrauschten Zustandes auf dem Purifikationsstrahlteiler. Konditioniert man auf der gequetschten Quadratur, tragen beide Terme zu einer Verkleinerung der Varianz V_{out} bei. Konditioniert man jedoch auf der antigequetschten Quadratur, konkurrieren die beiden Terme. In diesem Fall erfolgt die Reduzierung der Varianz V_{out} allein durch die Wirkungsweise des zweiten Terms (der erste Term ist dabei maximiert und B nimmt seinen

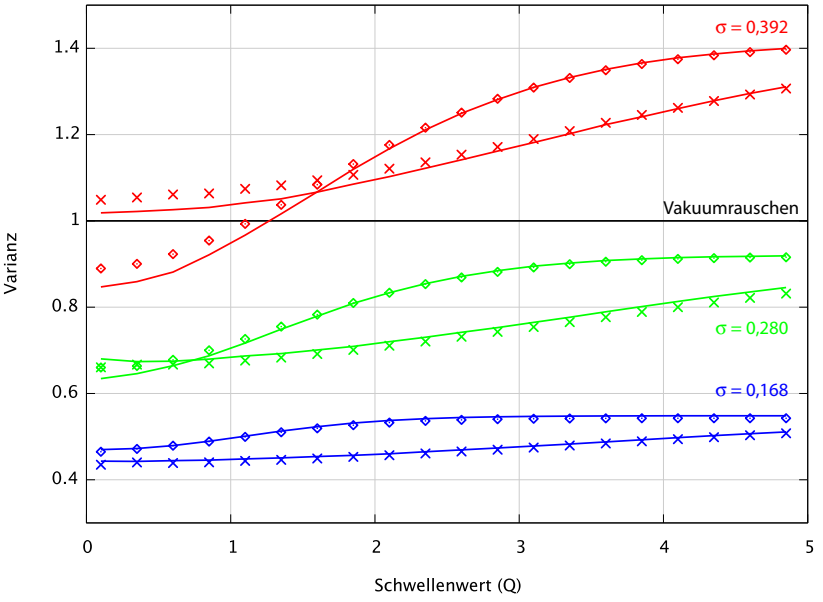

Abbildung 7.9 — Ausgabevarianzen von destillieren Zuständen über dem Schwellenwert Q. Es werden Ergebnisse jeweils für eine Konditionierung auf der ursprünglich gequetschten (Rauten) und auf der ursprünglich antigequetschten (Kreuze) Quadratur gezeigt. V_{out} ist dargestellt für drei verschiedene Phasenrauschstärken ($\sigma = 0{,}392$ (rot), $\sigma = 0{,}280$ (grün) und $\sigma = 0{,}168$ (blau)). Durchgezogene Linien zeigen wieder die Ergebnisse einer numerischen Simulation mit denselben Parametern.

maximalen Wert V_p an). Erstaunlicherweise ist der zweite Term hinreichend dominant um eine effektive Reduktion der Varianz von x_2 auch in diesem ungünstigsten Fall zu gewährleisten. Die Wirkungsweise dieses zweiten Terms beruht allein auf einer Quanteninterferenz an einem Strahlteiler.

Tatsächlich wird unter Anwendung des Destillationsprotokolls die Varianz *beider* Quadraturen x_2 und p_2 reduziert. Dies wird offenbar, wenn man das Unschärfeprodukt $U = \sqrt{V_x V_p}$ betrachtet. Das Unschärfeprodukt ist über dem Schwellenwert in ⇝Abbildung 7.8 gezeigt. Die gleichzeitige Unterdrückung der Fluktuationen in beiden Quadraturen ist dabei ein starker Beleg für eine zunehmende Reinheit des Zustandes unter der Destillation. Für gaußsche Zustände definiert man die Reinheit als $P = 1/U$. Für nicht zu starkes Phasenrauschen sind die verwendeten Zustände *gaußähnlich*.

In ⇝Abbildung 7.9 stellen wir (analog zu ⇝Abbildung 7.3) die Ausgabe-

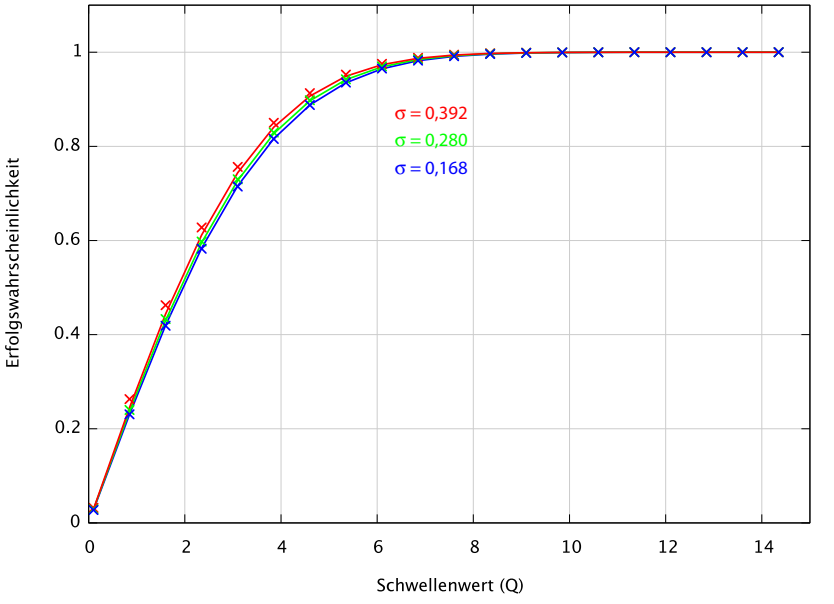

Abbildung 7.10 — Darstellung der Erfolgswahrscheinlichkeit über dem Schwellenwert beim Konditionieren auf der antigequetschten Quadratur. Wie erwartet weicht diese darstellung von der entsprechenden Abbildung im Falle einer Konditionierung auf der ursprünglich gequetschten Quadratur ab. Der Zusammenhang ist für drei verschiedene Stärken des Phasenrauschens gezeigt.

varianzen V_{out} über dem Schwellenwert dar. Dabei wird die Konditionierung auf der ursprünglich gequetschten (einfache Purifikation) und antigequetschten (*conjugate purification*) Quadratur gegenüber gestellt. Man beachte, dass für kleine Phasenrauschstärken die Konditionierung auf der antigequetschten Quadratur sogar effektiver ist, als eine Konditionierung auf der gequetschten. Die Erfolgswahrscheinlichkeit P wächst monoton mit steigendem Schwellenwert Q, hängt aber auch von der Wahl der Konditionierungsquadratur ab (vergleiche ⇝Abbildung 7.10).

In ⇝Abbildung 7.11 betrachten wir dieselben Daten, diesmal aufgetragen über der Erfolgswahrscheinlichkeit. Für kleine Phasenrauschstärken kann auch in dieser Darstellung ein Vorteil beim Konditionieren auf der antigequetschten Quadratur gefunden werden. Man beachte außerdem, dass wieder bereits für Erfolgswahrscheinkeiten von 0,3 bis 0,5 eine erhebliche Destillation bewerkstelligt werden kann. Eine weitere Verkleinerung der Erfolgswahrscheinlichkeit (etsprechend einer kleineren Wahl des Schwellenwertes) ergibt

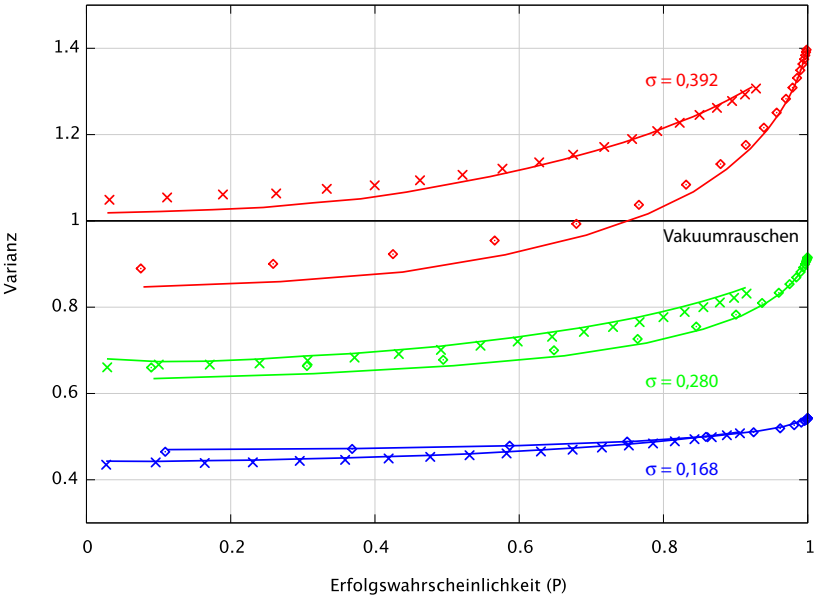

Abbildung 7.11 — Dieselben Daten wie zuvor für die Destillation bei Konditionierung auf gequetschter (Rauten) und antigequetschter (Kreuze) Quadratur, diesmal über der Erfolgswahrscheinlichkeit dargestellt. Die Abbildung zeigt deutlich, wie für kleines Phasenrauschen (blau) eine Konditionierung auf der antigequetschten Quadratur eine effizientere Destillation erlaubt, als eine Konditionierung auf der gequetschten Quadratur.

nur noch eine geringfügige weitere Verkleinerung der Ausgabevarianz V_{out}.

7.3 Konditionierung auf beliebiger und zufälliger Quadratur

Wir betrachten nun die Generierung eines Konditionierungssignals auf einer *beliebigen* Qudratur $q(\theta)$ und untersuchen die Abhängigkeit des Destillationsprotokolls von der Wahl der Quadratur. ⇝Abbildung 7.13 zeigt, dass es in der Tat keinen erheblichen Unterschied macht, welche Quadratur zur Konditionierung vermessen wird. Für die gewählten Parameter zeigt die Abbildung ein Minimum bei $\theta = 0$. Man beachte jedoch, dass ein tieferes Minimum im Fall $\theta = \pi/2$ voliegt. Für die gewählten Parameter erhält man also eine

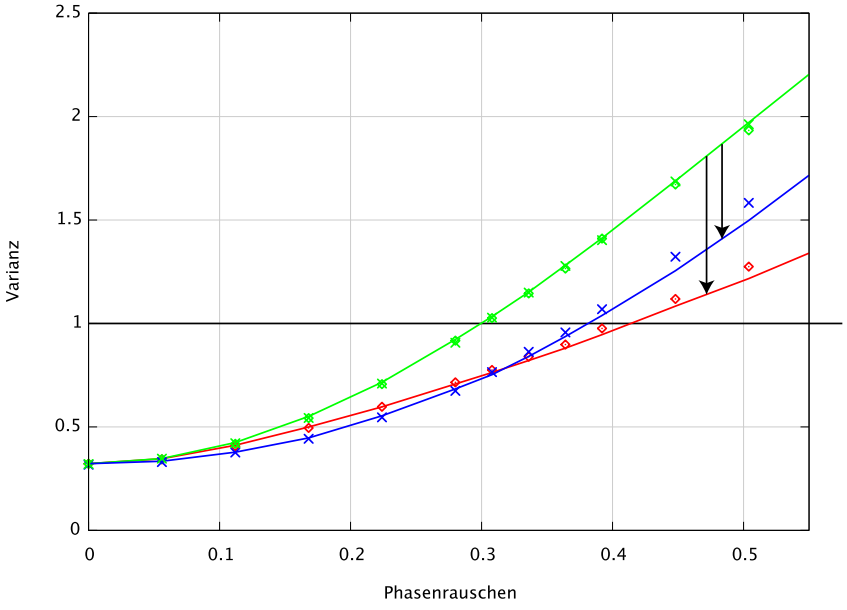

Abbildung 7.12 — Zusammenstellung der Ergebnisse von einfacher Destillation und Conjugate Purification. Dargestellt sind jeweils gemessene und simulierte Varianzen vor (grün) und nach (blau/rot) Anwendung des Destillationsprotokolls über der Stärke des Phasenrauschens σ. Die rote Kurve zeigt das Ergebnis, wenn auf die ursprünglich gequetschte Quadratur konditioniert wird $|x_1| < Q$, die grüne Kurve ergibt sich bei Konditionierung auf die ursprünglich antigequetschte Quadratur $|p_1| < Q$. Der Schwellenwert ist für diese Darstellung zu $Q = 1$ gewählt worden. Für nicht zu großes Phasenrauschen (ca. $\sigma < 0{,}3$) ist die Konditionierung auf die ursprünglich antigequetschte Quadratur effektiver. Man beachte wiederum, dass es mit beiden Strategien möglich ist, die Fluktuationen eines Zustandes unter das Vakuumrauschen zu bringen!

optimale Destillation, wenn die antigequetschte Quadratur $q(\pi/2) = p$ zur Konditionierung gewählt wird. Entscheidend ist die Beobachtung, dass die Fluktuationen des Ausgabezustandes für *jede* Wahl von θ reduziert wird!

Dies impliziert, dass eine Destillation auch dann stattfindet, wenn die vom Homodyndetektor vermessene Phase nicht kontrolliert wird und der Detektionswinkel frei driftet. In Form einer Simulation sind diese Umstände in ⇝Abbildung 7.14 umgesetzt. Man erkennt, dass bei nicht zu klein gewähltem Schwellenwert ein frei driftender Homodyndetektor eine effizientere Destillation ermöglicht, als dies bei kontrolliertem Homodyndetektor der Fall

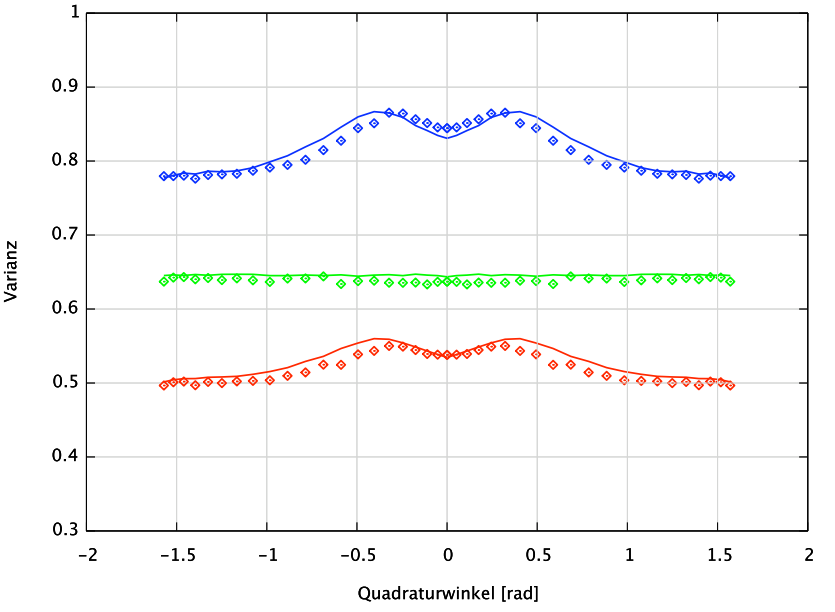

Abbildung 7.13 — Experimentelle und theoretische Ergebnisse des Destillationsprotokolls bei Konditionierung auf unterschiedliche Quadraturen $q_1(\theta)$ für festes Phasenrauschen $\sigma = 0{,}202$ und festen Schwellenwert $Q = 0{,}7$. Die grünen Daten zeigen die Varianz des nicht destillieren, phasenverrauschten Eingabezustandes. Die roten Daten erhält man, indem das Destillationsprotokoll angewendet wird (V_{out}). Für die hier gewählten Parameter arbeitet das Protokoll bei Konditionierung auf die ursprünglich gequetschte Quadratur effektiver. Allerdings findet eine Destillation bei *jeder* Wahl des Quadraturwinkel statt.

ist. Wählt man den Schwellenwert Q dagegen klein, so hängt es stark von der Stärke des vorhandenen Phasenrauschens ab, ob ein kontrollierter oder ein unkontrollierter Detektor die effizientere Destillation liefert.

7.4 Quantum Channel Probing

Wir hatten in den vorangegangenen Abschnitten verschiedene Strategien untersucht, eine Destillation und Purifikation phasenverrauschter Zustände durchzuführen. Dabei hatten wir uns vor allem mit unterschiedlichen Möglichkeiten befaßt, eine Konditionierung vorzunehmen.

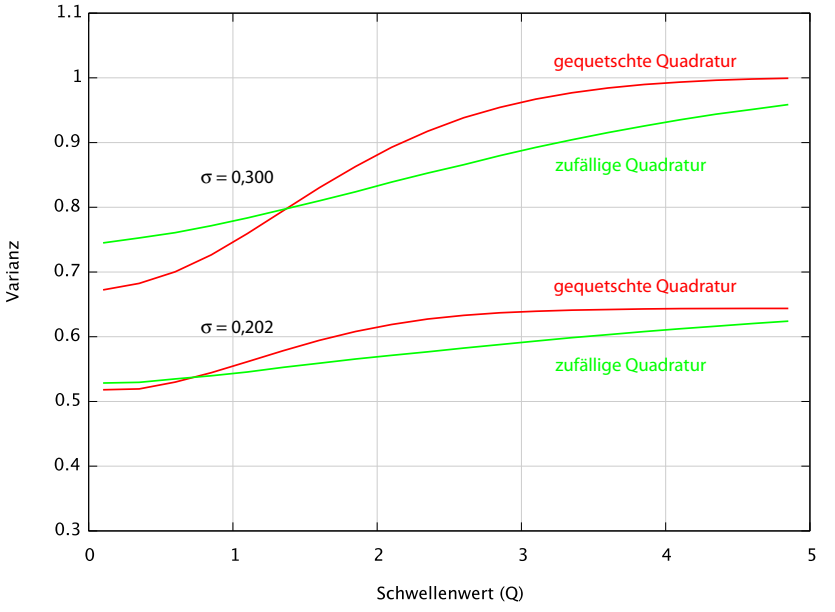

Abbildung 7.14 — Wirkung des Destillationsprotokolls bei für jede Konditionierung *zufällig* gewähltem Quadraturwinkel (grün) und bei Konditionierung auf der ursprünglich gequetschten Quadratur x_1. Für nicht zu kleine Schwellenwerte Q (der genau Wert von Q ist eine Funktion von σ), ist eine zufällig gewählte Konditionierungsquadratur effektiver. Dargestellt sind zwei verschiedene Werte des Phasenrauschens, nämlich $\sigma = 0{,}202$ (unteres Kurvenpaar) und $\sigma = 0{,}30$ (oberes Kurvenpaar).

Zusätzlich zu den bereits vorgestellten Verfahren kann auch klassische Information über den Übertragungskanal genutzt werden, um die Effektivität des Destillationsprotokolls zu steigern. Solche klassische Information über den Kanal kann mit dem Verfahren des *quantum channel probing* (QCP) ausgelesen werden.

Wir verwenden die Tatsache, dass *viele* Kopien der Zustände über den rauschbehafteten Kanal übertragen werden. Ein Teil dieser Zustände könnte also dazu verwendet werden, Informationen über den Kanal zu erhalten. Mit diesem Vorgehen kann die Effizienz des Destillationsprotokolls verbessert werden, falls das Phasenrauschen (oder ein Anteil davon) bei Frequenzen vorliegt, die kleiner sind als die Auflösebandbreite (*resolution bandwidth*, RBW), mit der die Messung erfolgt, im hier betrachteten Fall also 100 kHz. In diesem Fall sind die Phasenverschiebungen zweier aufeinander folgend gemessener

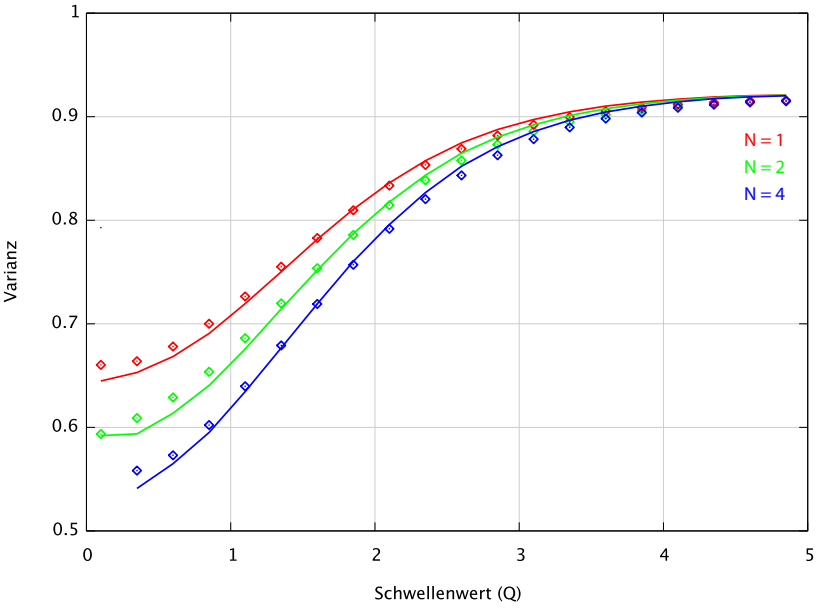

Abbildung 7.15 — Effekt des Quantum Channel Probing auf einen Zustand mit $\sigma = 0{,}28$ bei Verwendung von $N = 1$, $N = 2$ und $N = 4$ aufeinander folgenden Messwerten zur Konditionierung.

Zustände nicht völlig voneinander unabhängig. Das im folgenden vorgestellte und umgesetzte Protokoll nutzt genau diese Korrelation zwischen aufeinander folgend gemessenen Zuständen.

Beim *quantum chanel probing* wird ein Zustand nicht dann akzeptiert, wenn lediglich ein korrespondierender Messwert kleiner ist als ein Schwellenwert Q, sondern wenn dies für *eine Anzahl* N_{QCP} *aufeinander folgender Messwerte* gilt. In diesem Fall erhält man für die Ausgabevarianz den Ausdruck [Hag07]:

$$V_{\mathrm{out}} = \frac{1}{\mathcal{P}_{\mathrm{QCP}}} \int_{\phi_1} \int_{\phi_2} \left[B\,\mathrm{erf}\left(\frac{Q}{\sqrt{2A}}\right) - \sqrt{\frac{2}{\pi}} \frac{C^2 Q}{A^{3/2}} e^{-\frac{Q^2}{2A}} \right] \times \tag{7.16}$$

$$\left[\mathrm{erf}\left(\frac{Q}{\sqrt{2A}}\right)\right]^{N_{\mathrm{QCP}}-1} \Phi(\phi_1)\Phi(\phi_2)\,d\phi_1 d\phi_2, \tag{7.17}$$

wobei $\mathcal{P}_{\mathrm{QCP}}$ wieder die Erfolgswahrscheinlichkeit

$$\mathcal{P}_{\mathrm{QCP}} = \int_{\phi_1} \int_{\phi_2} \left[\mathrm{erf}\left(\frac{Q}{\sqrt{2A}}\right)\right]^{N_{\mathrm{QCP}}} \Phi(\phi_1)\Phi(\phi_2)\,d\phi_1 d\phi_2 \tag{7.18}$$

ist. Der Effekt des QCP wird also durch zusätzliche Faktoren $[\mathrm{erf}(Q/\sqrt{2A})]$ repräsentiert. Wird als Quadratur $q(\theta)$ die ursprünglich gequetschte Quadratur $q_1(0) = x_1$ gewählt, so ist dieses Protokoll äquivalent zu einem Auslesen der Ausrichtung der Quetschellipsen, denn das Bestehen des Kriteriums $|x_1| < Q$ für mehr als einen nacheinander erhaltenen Messwert ist wahrscheinlicher, wenn die schmalen Halbachsen der Ellipsen in der vermessenen Quadratur liegen. In allen Fällen wurde auf die ursprünglich gequetschte Quadratur konditioniert. Die ⇝Abbildung 7.15 zeigt die Ergebnisse (gemessen und simuliert) bei Anwendung von QCP für die Fälle $N_{\mathrm{QCP}} = 2$ und $N_{\mathrm{QCP}} = 4$ im Vergleich mit dem vorher bereits betrachteten Fall $N_{\mathrm{QCP}} = 1$. Abbildung 7.16 zeigt dieselben Daten, diesmal aufgetragen über der Erfolgswahrscheinlichkeit. Aus ⇝Abbildung 7.17 erkennt man, dass bei Implementierung von QCP die Erfolgswahrscheinlichkeit für einen fest gewählten Schwellenwert Q dramatisch abnimmt. Demgegenüber stehen Verkleinerungen der Varianz V_{out}, die ohne Anwendung von QCP gar nicht erreichbar sind. Die Anwendung von QCP bringt keine Verbesserung, wenn auf die ursprünglich antigequetschte Quadratur konditioniert wird. Dies ist verständlich, denn in diesem Fall arbeitet der Effekt des negativen *conjugate purification*-Terms genau gegen den Effekt des QCP.

QCP stellt also eine effektive Erweiterung eines einfachen Purifikationsprotokolles dar. Voraussetzung für das Funktionieren von QCP ist der Umstand, dass das Phasenrauschen, welches die Kopien eines Zustandes erleiden (ganz oder teilweise) innerhalb der Auflösebandbreite vorliegt, mit der die Messung erfolgt. Ist dies nicht der Fall, besteht die ausgenutze Korrelation zwischen aufeinander folgend erfaßten Messwerten nicht. In jedem realistischen Szenario wird man stark bemüht sein, die Auflösebandbreite so hoch wie möglich zu setzen, da damit ein Gewinn an Bandbreite einhergeht. Damit wird man schnell ein Regime erreichen, bei dem ein großer Anteil des Phasenrauschens bei solchen kleinen Frequenzen (verglichen mit der Auflösebandbreite) vorhanden ist, so dass QCP eine sinnvolle Erweiterung des Purifikationsprotokolls darstellt.

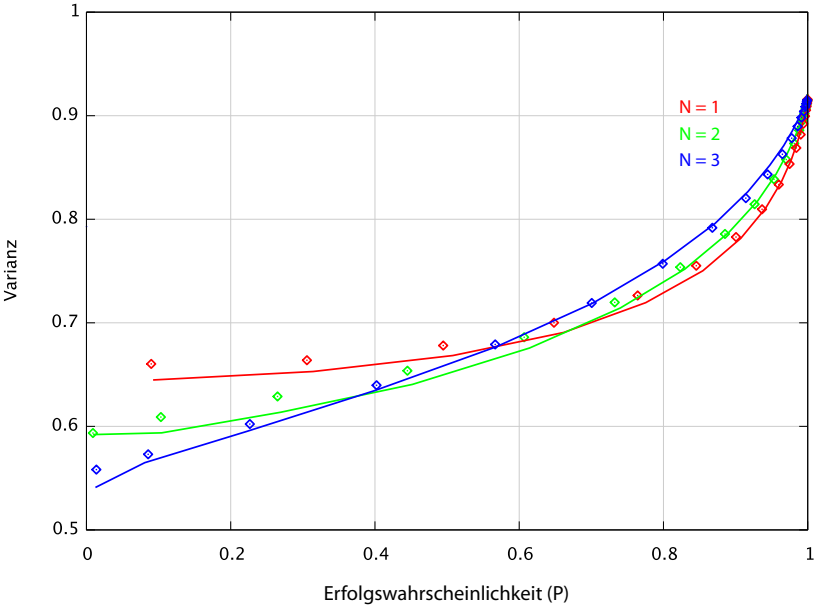

Abbildung 7.16 — Dieselben Daten wie zuvor (⇝Abbildung 7.15), diesmal dargestellt über der Erfolgswahrscheinlichkeit $\mathcal{P}$.

7.5 Einfluss der Phasenrauschcharakteristik

Wir hatten bei allen bisherigen Betrachtungen vorausgesetzt, dass das Phasenrauschen, welchem die zu übertragenden Zustände unterworfen werden, eine gaußsche Verteilung aufweist:

$$\Phi(\phi) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\phi^2}{2\sigma^2}\right). \tag{7.19}$$

Diese Annahme wurde motiviert durch die technische Einfachheit einer solchen Verteilung bei der analytischen Betrachtung und gerechtfertigt durch die Annahme, dass das Rauschen bei einer realen Übertragung durch einen *langen* optischen Kanal ($l \approx 10^3$ m) eine Normalverteilung aufweist.

Die Annahme einer gaußschen Verteilung des Rauschens schränkt erstaunlicherweise die Funktionsfähigkeit des Destillationsprotokolls in keiner Weise ein. Nimmt man zum Beispiel an, dass das Rauschen tatsächlich einer anderen Verteilung folgt (zum Beispiel einer Gleichverteilung), kann man sich durch

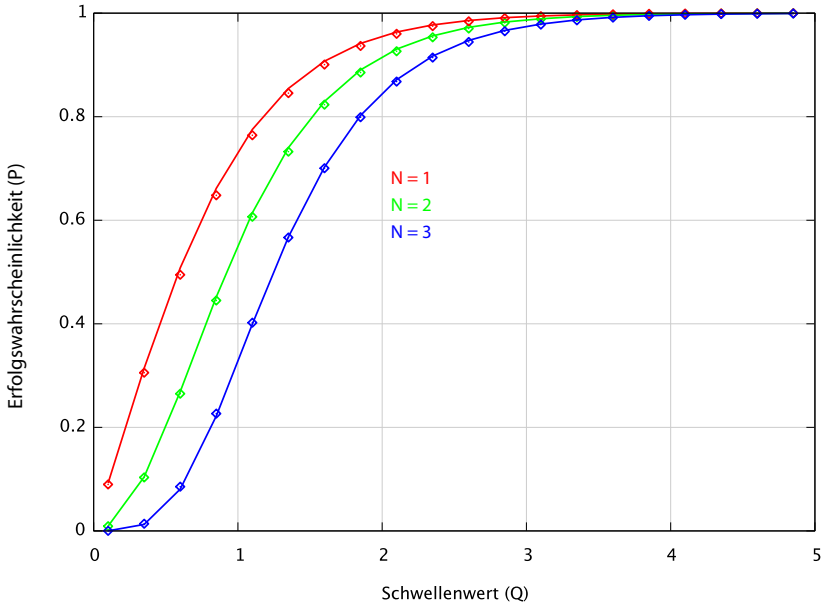

Abbildung 7.17 — Zusammenhang zwischen Schwellenwert Q und Erfolgswahrscheinlichkeit P beim Quantum Channel Probing für $N = 1$, $N = 2$ und $N = 4$. Man beachte, wie mit steigendem N die Erfolgswahrscheinlichkeit dramatisch abnimmt!

numerische Simulation davon überzeugen, dass die Effizienz des Protokolls dadurch nicht beeinträchtigt wird (⇝Abbildung 7.18). Bei einer realen Implementation des Verfahrens ist also keine Kenntnis der Rauschverteilung vorauszusetzen, was eine solche Implementation erheblich vereinfacht.

7.6 Multi-Kopien-Destillation

Nach der Darstellung der Ergebnisse zur Destillation von Squeezing bei Benutzung von zwei Kopien eines gequetschten Zustandes ist es ein naheliegender Ansatz zu fragen, ob das Destillationsprotokoll erweitert werden kann, wenn *mehr als zwei* Kopien verwendet werden. Man spricht dann von *Multi-Kopien-Destillation* oder auch von*iterativer Destillation* im weiteren Sinne.

Stehen drei Kopien zur Verfügung, kann ein Schema wie in ⇝Abbildung 7.19 durchgeführt werden. Dazu wird ein Ausgang des Purifikationsstrahlteilers mit der dritten Kopie eines gequetschten Zustandes an einem weiteren

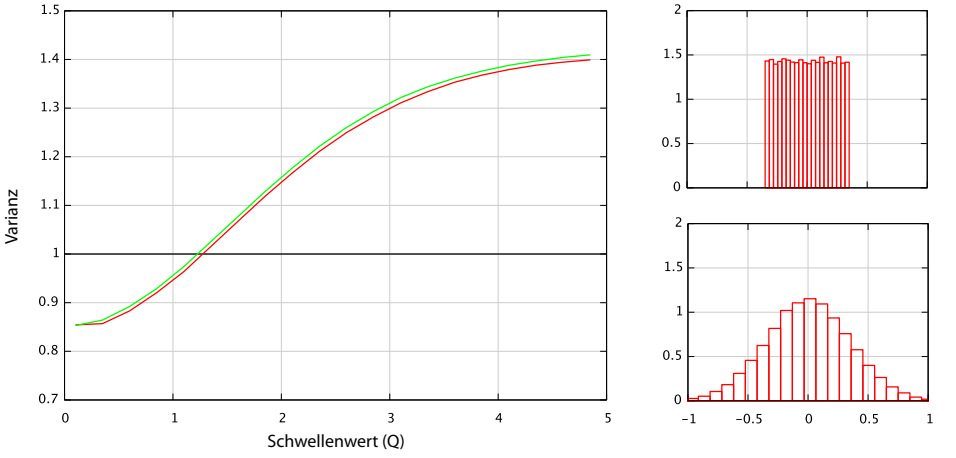

Abbildung 7.18 — Simulation des Destillationsprotokolls für Phasenrauschen unterschiedlicher Verteilung. Die rote Kurve ist die bereits bekannte Darstellung der Ausgabevarianz über dem Schwellenwert für den Fall eines normalverteilten Rauschens (siehe unteres Histogramm). Die grüne Kurve erhält man bei ansonsten unveränderten Parametern, wenn man stattdessen ein gleichverteiltes Rauschen (gleicher Standardabweichung σ) verwendet. Die resultierenden Kurven sind bis auf minimale Unterschiede im Rahmen der Rechengenauigkeit absolut identisch. Damit muss vor einem Hintergrund der technologischen Realisierung die Form des Rauschens nicht bedacht werden!

Purifikationsstrahlteiler überlagert. Der Zustand im einen Ausgang dieses zweiten Strahltreilers wird genau dann akzeptiert, wenn die *beiden* übrigen Zustände einer Konditionierungsbedingung genügen ($|x| < Q$ oder $|q(\theta)| < Q$).

Dasselbe Schema kann auch für eine beliebige Anzahl N von Kopien eines gequetschten Zustandes angewendet werden und wird allgemein als *kollektive Destillation* bezeichnet.

Für den Fall einer *geraden* Anzahl von Zuständen ist noch ein anderes Protokoll denkbar, das für den Spezialfall $N = 4$ ebenfalls in ⇝Abbildung 7.19 gezeigt ist. Dabei werden zunächst je zwei Zustände an je einem Strahlteiler überlagert. Jeweils einer der Ausgänge von jedem Strahlteiler wird mit einem Homodyndetektor registriert. Die beiden verbleibenden Ausgänge werden erneut an einem weiteren Strahlteiler überlagert. Von diesem wird ein Ausgang per Homodyndetektion vermessen. Man konditioniert nun derart, dass der Zustand im verbleibenden Ausgang akzeptiert wird, wenn alle drei Meßergebnisse der drei Detektoren einer Konditionierunngsbedingung der Form

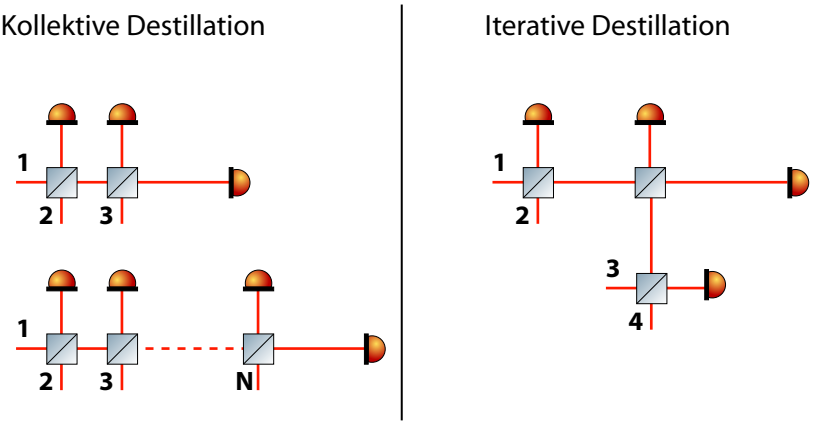

Abbildung 7.19 — Erweiterung des Destillationsprotokolls, wenn mehr als zwei Kopien zur Verfügung stehen. Kollektive Destillation kann für jede Anzahl N von Zuständen implementiert werden. Dabei wird je ein Ausgang jedes Purifikationsstrahlteilers mit einem Homodyndetektor vermessen. Der jeweils andere Ausgang wird erneut mit einer weiteren Kopie überlagert. Betrachtet man speziell die Fälle mit einer geraden Anzahl von Zuständen, kann iterative Destillation implementiert werden (rechts).

$|x| < Q$ genügen. Dieses kaskadierte Vorgehen wird als *iterative Purifikation* im eigentlichen Sinne bezeichnet.

Sowohl bei der kollektiven Destillation, als auch bei der iterativen Destillation werden für ein Protokoll, das N Kopien berücksicht, $N-1$ Purifikationsstrahlteiler verwendet.

Eine experimentelle Umsetzung dieser erweiterten Protokolle ist bisher nicht erfolgt und in unseren Augen auch nicht notwendig. Wir hatten gesehen, dass die durch Simulation erhaltenen Ergebnisse eine hervorragende Übereinstimmung mit den Meßergebnissen aufweisen. Die Charakteristika iterativer Protokolle sind sehr detailliert in [Mar07] untersucht und dargestellt. Wir zeigen an dieser Stelle lediglich ein einfaches Beispiel (Simulation) und fassen kurz die Ergebnisse aus [Mar07] zusammen. Wir betrachten speziell den Fall einer kollektiven Destillation. Für lediglich zwei Kopien ($N = 2$) geht diese über in das bisher dargestellte und untersuchte Schema. Wir vergleichen $N = 2$ mit dem Fall einer kollektiven Purification mit drei Kopien ($N = 3$). Simulierte Ergebnisse sind in ⇝Abbildung 7.20 dargestellt. Man kann sehen, dass bei Umsetzung von kollektiver Destillation mit $N = 3$ eine deutliche Steigerung der Effizienz des Destillationsprotokolls eintritt. Zusätzlich zur

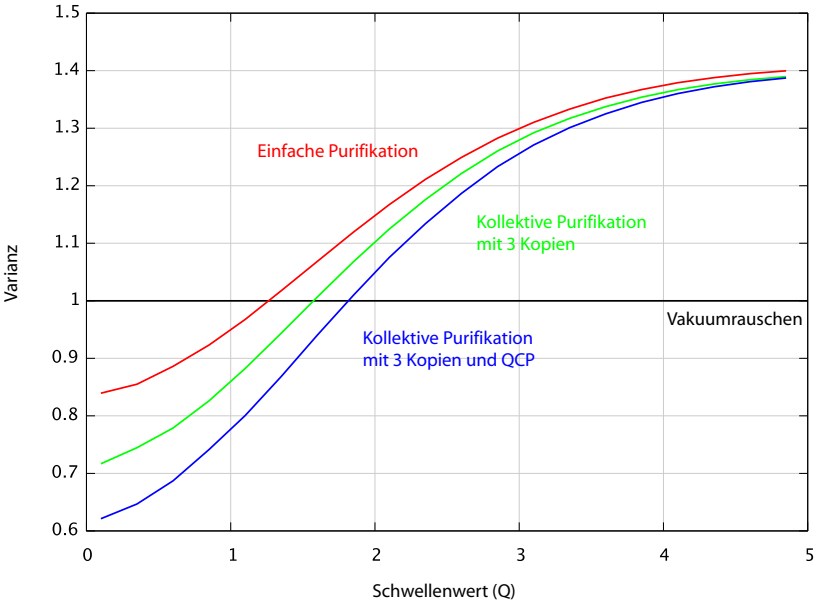

Abbildung 7.20 — Wirkungsweise verschiedener Destillationsstrategien. Die rote Kurve zeigt die Wirkung der einfachen Destillation bei Verwendung von zwei Kopien und Konditionierung auf der ursprünglich gequetschten Quadratur. Die grüne Kurve zeigt das Ergebnis einer kollektiven Destillation bei Verwendung von drei Kopien. Für die blaue Kurve ist zusätzlich zur kollektiven Destillation mit drei Kopien noch QCP mit $N_{\mathrm{QCP}} = 2$ implementiert worden.

kollektiven Destillation mit drei Kopien kann, wie bereits zuvor beschrieben, noch *quantum channel probing* implementiert werden. Die Ergebnisse für kollektive Destillation mit QCP ($N_{\mathrm{QCP}} = 2$) können ebenfalls in ⇝Abbildung 7.20 betrachtet werden.

Man beachte, dass bereits bei der Verwendung von nur drei Kopien ($N = 3$) und *quantum channel probing* mit $N_{\mathrm{QCP}} = 2$ eine nichtklassische Rauschunterdrückung von fast 3 dB zurückerhalten werden kann!

Bei Verwendung zusätzlicher Kopien bei der kollektiven Purifikation und einem höheren N_{QCP} beobachtet man eine weitere Effizienzsteigerung. Im asymtotischen Grenzfall kann ein großer Teil der ursprünglichen nichtklassische Rauschunterdrückung zurückerhalten werden (bei stetig abnehmender Erfolgsrate). Die Frage nach einer optimalen Strategie wird auch in [Mar07] behandelt.

KAPITEL 8

Bewertung und Ausblick

In diesem Kapitel wird das vorgestellte Protokoll zur Destillation und Purifikation gequetschter Zustände früheren Experimenten, vor allem solchen, die auf diskreten Variablen beruhen, gegenüber gestellt. Es folgt eine Darstellung der Kernergebnisse und ein Ausblick bezüglich der experimentellen Umsetzung eines Destillationsprotokolls für verschränke Zustände.

8.1 Vergleich mit früheren Experimenten im Regime diskreter Variablen

Wie wir gesehen haben, ist die Verteilung von verschränkten Paaren zwischen weit voneinander entfernten Kommunikationspartnern essentiell für die zukünftige Umsetzung quantengestützter Kommunikationsprotokolle. Aufgrund unausweichlicher Rauscheinflüsse gehen bei der Übertragung mit zunehmender Propagationslänge die nichtklassischen Eigenschaften der Zustände verloren. Die Umsetzbarkeit von quantengestützten Kommunikationsprotokollen hängt also unmittelbar von der Umsetzung eines Destillationsprotokolls für verschränkte Zustände ab.

Im Regime diskreter Variablen (Einzelphotonen, Qbits) ist von Bennett [Ben96] ein Protokoll zur Destillation verschränkter Zustände vorgeschlagen worden. Die Funktionsweise des Prokolls ist in ⇝Abbildung 8.1 dargestellt. Eine große Schwäche dieses Protokolls ist die Verwendung der logischen CNOT[1] -Operation. Obwohl einige Quanten-Logikgatter realisiert werden konnten

[1] Ein CNOT („Controlled NOT“, manchmal auch C-NOT) ist eine logische Operation, die

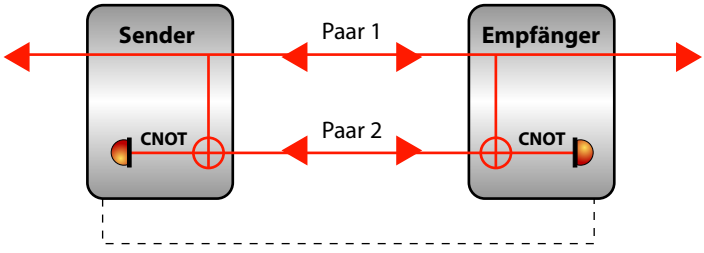

Abbildung 8.1 — Schematische Darstellung des von Bennett vorgeschlagenen Protokolls zur Destillation verschränkter Zustände. Aus zwei Paaren verschränkter Zustände soll ein einzelnes Paar mit einem höheren Grad an Verschränkung gewonnen werden. Dazu wird sowohl auf Seiten des Senders als auch auf Seiten des Empfängers eine CNOT-Operation durchgeführt. Anschließend vermessen beide den Zustand des Photons und vergleichen per klassischer Kommunikation. Im Fall übereinstimmender Meßergebnisse weist das verbleibende Photonenpaar einen höheren Grad von Verschränkung auf.

([Mon95]), existiert keine Demonstration einer CNOT-Operation, die vor einem realistischen Hintergrund im Rahmen einer Quantenkommunikation über große Distanzen angewendet werden könnte.

Bennetts Vorschlag ähnelnde Protokolle, die ohne eine CNOT-Operation auskommen, wurden für diskrete Variablen inzwischen umgesetzt [Pan01, Kwi01, Pan03, Yam03]. Beispielhaft soll die Funktionsweise des Protokolls aus [Pan01] dargestellt werden. Im Gegensatz zu Bennetts Vorschlag werden lediglich lineare optische Komponenten und klassische Kommunikation benötigt. Die beiden Werte eines Qbits (entsprechend den binären Symbolen „0“ und „1“) werden in einer Eigenschaft einzelner Photonen implementiert, z. B. der Polarisation. Ein Photon liegt demnach in einer der beiden orthogonalen Polarisationen $|H\rangle$ („horizontal“) oder $|V\rangle$ („vertikal“) vor.

Ziel von Sender („S“) und Empfänger („E“) ist es, verschränkte Photonenpaare zu teilen, die sich in dem maximal verschränkten Zustand

$$|\phi^+\rangle_{\mathrm{SE}} = \frac{1}{\sqrt{2}} \left(|H\rangle_{\mathrm{S}} |H\rangle_{\mathrm{E}} + |V\rangle_{\mathrm{S}} |V\rangle_{\mathrm{E}} \right) \tag{8.1}$$

das zweite Qbit eines Paares umdreht, wenn das erste Qbit (das „control bit“) des Paares den Wert „1“ hat. Also: $00 \to 00$, $01 \to 01$, $10 \to 11$, $11 \to 10$.

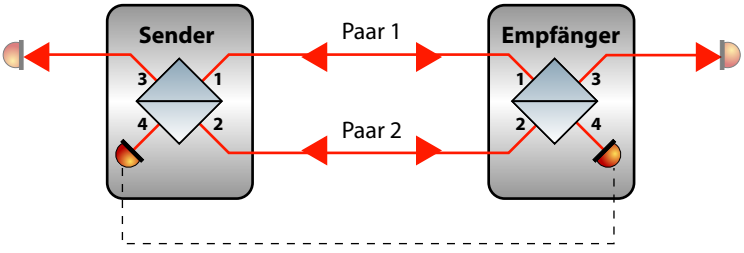

Abbildung 8.2 — Ein abgewandeltes Protokoll zur Destillation verschränkter Zustände. Die CNOT-Operationen aus Bennetts Vorschlag werden durch je einen Polarisationsstrahlteiler ersetzt.

befinden. Zu diesem Zweck werden in einer Quelle verschränkte Photonenpaare erzeugt und zwischen Sender und Empfänger aufgeteilt. Durch den unvermeidlichen Einfluss der Dekohärenz während der Übertragung gehen diese Zustände in den gemischten Zustand

$$\rho_{\mathrm{SE}} = F \left|\phi^+\right\rangle_{\mathrm{SE}} \left\langle\phi^+\right| + (1-F) \left|\psi^+\right\rangle_{\mathrm{SE}} \left\langle\psi^+\right| \tag{8.2}$$

über, wobei

$$\left|\psi^+\right\rangle_{\mathrm{SE}} = \frac{1}{\sqrt{2}} \left[|H\rangle_{\mathrm{S}} |V\rangle_{\mathrm{E}} + |V\rangle_{\mathrm{S}} |H\rangle_{\mathrm{E}}\right] \tag{8.3}$$

ist, also eine Mischung mit dem unerwünschten Zustand $\left|\psi^+\right\rangle_{\mathrm{SE}}$ stattgefunden hat. (Die explizite Form von $\left|\psi^+\right\rangle_{\mathrm{SE}}$ dient lediglich als Beispiel. Man kann die allgemeine Gültigkeit des Protokolls zeigen.) Zur Konstruktion eines Destillationsprotokolls wird nun gegenüber Bennetts Vorschlag jedes CNOT-Gatter durch einen Polarisationsstrahlteiler ersetzt (⇝Abbildung 8.2). Zur Wirkungsweise von Polarisationsstrahlteilern auf einzelne Photonen betrachte man ⇝Abbildung 8.3.

Das Destillationsprotokoll kommt nun dadurch zustande, dass man genau die Fälle selektiert, in denen sich genau *ein Photon* in *jedem der vier* Ein- und Ausgänge der Polarisationsstrahlteiler befindet (sogenannter *„4-mode-case“*). Hierzu ist es notwendig, in allen vier Ausgängen der beiden Strahlteiler eine Einzelphotonendetektion durchzuführen.

Aus ⇝Gleichung (8.2) liest man ab, dass der Gesamtzustand der beiden Paare (der Benennung der Strahlteilereingänge aus ⇝Abbildung 8.3 folgend

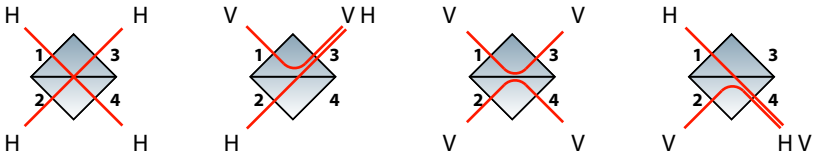

Abbildung 8.3 — Wirkungsweise eines Polarisationsstrahlteilers auf Einzelphotonen. Der Strahlteiler transmittiert horizontale Polarisation und reflektiert vertikale Polarisation. Die beiden Eingänge des Strahlteilers sind mit „1“ und „2“ bezeichnet, „3“ und „4“ benennt folglich die beiden Ausgänge. Genau in den Fällen, in denen die beiden einfallenden Photonen die gleiche Polarisation aufweisen, werden beide Ausgänge des Strahlteilers von einem Photon belegt.

als „1“ und „2“ bezeichnet) als gewichtete Mischung von vier Zuständen angesehen werden kann: Mit einer Wahrscheinlichkeit von F^2 findet man die Paare „1“ und „2“ in dem Zustand

$$|\phi^+\rangle_{\mathrm{S1E1}} |\phi^+\rangle_{\mathrm{S2E2}}, \tag{8.4}$$

mit Wahrscheinlichkeit $F(1-F)$ in einem der Zustände

$$|\phi^+\rangle_{\mathrm{S1E1}} |\psi^+\rangle_{\mathrm{S2E2}} \quad \text{oder} \quad |\psi^+\rangle_{\mathrm{S1E1}} |\phi^+\rangle_{S2E2} \tag{8.5}$$

und mit Wahrscheinlichkeit $(1-F)^2$ in dem Zustand

$$|\psi^+\rangle_{\mathrm{S1E1}} |\psi^+\rangle_{\mathrm{S2E2}}. \tag{8.6}$$

Man mache sich nun klar, dass die beiden „Mischzustände“ aus ⇝Gleichung (8.5) niemals zu der oben beschriebenen Situation führen, dass alle vier Ein- und Ausgänge der Polarisationsstrahlteiler von genau einem Photon besetzt werden: Sind die Polarisationen zweier Photonen auf Seiten des Senders gleich, so sind sie beim Empfänger verschieden, und umgekehrt.

Wir betrachten nun die beiden verbleibenden Fälle. Liegt der Zustand ⇝Gleichung (8.4) vor, erhalten Sender und Empfänger den Ausgabezustand $|\phi^+\rangle_{\mathrm{S3E3}}$ genau dann, wenn in jedem Strahlteilerausgang ein Photon vorhanden ist, also in 50% der Fälle. Im Fall ⇝Gleichung (8.6) erhalten Sender und Empfänger in der Hälfte der Fälle den Ausgabezustand $|\psi^+\rangle_{\mathrm{S3E3}}$.

Zusammenfassend stellt man also fest, dass Sender und Empfänger den Zustand $|\phi^+\rangle_{\mathrm{S3E3}}$ mit einer Wahrscheinlichkeit $F^2/2$ und den Zustand $|\psi^+\rangle_{\mathrm{S3E3}}$ mit einer Wahrscheinlichkeit $(1-F)^2/2$ erhalten. Unter Anwendung des Destillationsprotokolls wird also ein neues Ensemble

$$\rho'_{\mathrm{SE}} = F' \left|\phi^+\right\rangle_{\mathrm{SE}} \left\langle\phi^+\right| + (1-F') \left|\psi^+\right\rangle_{\mathrm{SE}} \left\langle\psi^+\right| \tag{8.7}$$

präpariert mit einem Anteil

$$F' = \frac{F^2}{F^2 + (1-F)^2} > F \qquad (F > 1/2) \tag{8.8}$$

des gewünschten Zustandes $|\phi^+\rangle_{\mathrm{SE}}$, der größer ist als der Anteil F vor der Anwendung des Protokolls.

Das beschriebene Protokoll hat, verglichen mit Bennetts ursprünglichem Vorschlag, zwei gravierende Nachteile: Die Erfolgswahrscheinlichkeit ist um einen Faktor Zwei geringer. An ⇝Gleichung (8.8) liest man außerdem ab, dass für den Anteil des gewünschten Zustandes F gelten muss:

$$F > \frac{1}{2}. \tag{8.9}$$

Das Protokoll wird also mit zunehmender Verunreinigung des ursprünglichen Zustandes zunehmend ineffektiver und versagt für $F < 1/2$ vollständig. Zusätzlich zu diesen prinzipiellen Beschränkungen des Protokolls muss erneut auf die Notwendigkeit der Einzelphotonendetektion hingewiesen werden, die nach wie vor nicht mit befriedigend hoher Effizienz erledigt werden kann. Damit ist die Anwendbarkeit eines solchen Protokolls vor dem Hintergrund einer technologischen Realisierung eines Quanteninformationsprotokolls stark eingeschränkt und kann nicht mit Protokollen im Regime kontinuierlicher Variablen konkurrieren. Insbesondere erfordert das Protokoll eine Detektion in allen vier Ausgängen der beiden Strahlteiler, um die *4-mode-cases* zu selektieren. Damit wird zwar ein Subensemble der beteiligten Photonen identifiziert, das einem destillierten Zustand entspricht, jedoch nicht präpariert, also nicht für Folgeanwendungen zur Verfügung gestellt.

8.2 Zusammenfassung

Vor allem im Hinblick auf eine technologische Realisierung in einem realistischen Szenario stellen kontinuierliche Variablen bei der Umsetzung von

Quanteninformationsprotokollen eine ansprechende Alternative zu diskreten Variablen dar. Der Vorteil des Regimes diskreter Variablen liegt allein in der direkten Analogie zwischen Qbits und klassischen Bits. Damit ist die Tatsache verständlich, dass in der historischen Entwicklung der Quanteninformationstheorie zunächst diskrete Variablen betrachtet worden sind.

Denkt man über eine technologische Implemtierung solcher Protokolle nach, sind kontinuierliche Variablen dem traditionellen Ansatz, der diskrete Variablen betrachtet, in allen praktisch relevanten Aspekten (Verfügbarkeit der benötigten Komponenten, erzielbare Effizienzen und Bandbreiten, Schwierigkeit von Erzeugung und Detektion, ...) weit überlegen.

Als entscheidend wichtige Vorstufe zum ambitionierten Vorhaben der Umsetzung eines Destillationsprotokolls für verschränkte Zustände im Regime kontinuierlicher Variablen ist der Gegenstand der vorliegenden Arbeit die experimentelle und theoretische Untersuchung eines Destillationsprotokolls für gequetschten Zustände.

Bei der Verteilung nichtklassischer (gequetschter oder verschränkter) Zustände zwischen räumlich weit entfernten Kommunikationspartnern werden die nichtklassischen Eigenschaften durch Störungseffekte des optischen Übertragungskanals erheblich beeinträchtigt. Ein Destillationsprotokoll begegnet dieser Tatsache mit dem Ansatz aus einer großen Anzahl schwach nichtklassischer Zustände eine kleinere Anzahl von Zuständen mit großer Nichtklassizität zu gewinnen. Die Stärke der Nichtklassizität wird dabei mit der Stärke der nichtklassischen Rauschunterdrückung identifiziert.

Ein zunächst naiv erscheinender Ansatz zur Verwirklichung eines Destillationsprotokolls besteht darin, zwei Kopien eines gequetschten Zustandes zu erzeugen, über einen optischen Kanal zu übertragen (wodurch die nichtklassische Rauschunterdrückung erheblich vermindert wird) und aus diesen beiden Zuständen einen einzelnen Zustand nun wieder größerer Rauschunterdrückung zu erzeugen. Zur Nachbildung der Übertragung eines optischen Kanals wurden die beiden Kopien eines gequetschten Zustandes mit zufälligem, in einem Frequenzband weißen und mit gaußförmiger Gewichtung ausgestattetem Phasenrauschen versehen. (Die genaue Form des Rauschens spielt für die Funktion des Protokolls keine Rolle).

Eine Destillation gelingt durch phasenstarre und modenangepasste Überlagerung der beiden Zustände auf einem Strahlteiler. Einer der Ausgänge des Strahlteilers wird mit einem Homodyndetektor vermessen und der Zustand im zweiten Ausgang des Strahlteilers wird „akzeptiert“, falls der Messwert des Homodyndetektors einem Konditionierungskriterium der Form $|x| < Q$ (für einen fest gewählten Schwellenwert Q) genügt. Wird das Kriterium nicht

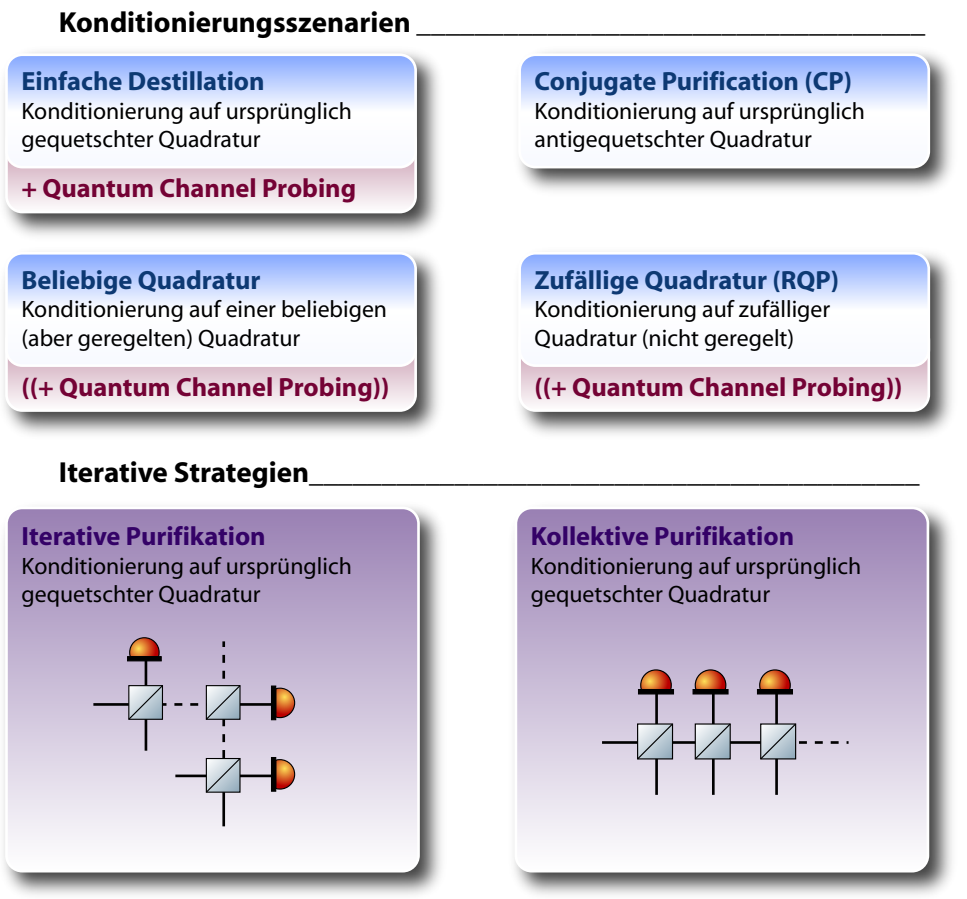

Abbildung 8.4 — Übersicht über die Nomenklatur der unterschiedlichen Strategien und Erweiterungen für Destillationsprotokolle.

erfüllt, so wird der Zustand „abgelehnt“.

Es konnte gezeigt werden, dass durch ein solches Vorgehen tatsächlich ein Destillationsprotokoll realisiert wird. Experimentell gewonnene Daten zeigten dabei eine hervorragende Übereinstimmung mit ebenfalls durchgeführten numerischen Simulationen. Unter der Anwendung dieses Protkolls wird nicht nur der Grad der nichtklassischen Rauschunterdrückung reduziert („Destillations“), sondern auch die Reinheit des Zustandes vergrößert („Purifikation“). Außerdem wird die Messstatistik der Zustände gaußförmiger („Gaußifikation“). Mit diesen Ergebnissen wurde die zum Zeitpunkt der Durchführung

vorliegende Theorie in vollem Umfang bestätigt.

Im nächsten Schritt konnte demonstriert werden, dass eine Destillation des Quetschgrades auch dann stattfindet, wenn von einem Homodyndetektor *nicht* die ursprünglich gequetschte Quadratur x, sondern die ursprünglich antigequetschte Quadratur p vermessen wird, also eine Konditionierung der Form $|p| < Q$ vorgenommen wird. Erstaunlicherweise gibt es ein Regime der Stärke des Phasenrauschens, in dem diese *conjugate purification* sogar effektiver arbeitet, als eine Konditionierung auf der ursprünglich gequetschten Quadratur. Durch numerische Simulation wurde gezeigt, dass dieser Effekt in der bestehenden Theorie – bisher unerkannt – enthalten war.

Es wurde dann die Vermutung experimentell und numerisch bestätigt, dass eine Destillation auch dann stattfindet, wenn auf eine beliebige Quadratur $q(\theta)$ konditioniert wird. Es wurde außerdem der Fall betrachtet, dass die vermessene Quadratur nicht geregelt wird, also frei driftet. Auch in diesem Fall fand eine Destillation des Quetschgrades statt.

Als Erweiterung des bisherigen Destillationsprotokolls wurde *quantum channel probing* (QCP) entwickelt und experimentell demonstriert. Im Falle einer Konditionierung auf der ursprünglich gequetschten Quadratur kann mit QCP eine weitere deutliche Verbesserung der Destillationseffizienz (auf Kosten der Erfolgsrate) bewerkstelligt werden. Im Falle der Durchführung von *conjugate purification* ist QCP kein geeignetes Werkzeug zur Verbesserung der Effizienz.

Zuletzt wurde kurz auf die Möglichkeiten einer iterativen Anwendung des Destillationsprotkolls hingewiesen, d. h. einer Erweiterung des bestehenden Protokolls für den Fall, dass mehr als zwei Kopien eines gequetschten Zustandes zur Verfügung stehen. Abhängig von der Anzahl der Kopien können zwei Strategien eines iterativen Protokolls angewendet werden, nämlich *iterative Destillation* (im eigentlichen Sinne) und *kollektive Destillation*. Im Falle kollektiver Destillation ist wiederum QCP als wirkungsvolles Mittel zur Effizienzsteigerung demonstriert worden. Eine Übersicht über die verschiedenen Strategien zur Destillation gequetschter Zustände findet man in ⇝Abbildung 8.4.

8.3 Ausblick

Quantenmechanische Verschränkung ist die wichtigste Grundlage für viele Anwendungen in der Quantenkommunikation und -information. Beginnend

mit der erfolgreichen Demonstration von Quantenteleportation 1998 [Fur98] ist die Umsetzung von Quanteninformationsprotokollen mit kontinuierlichen Variablen in den Blickpunkt theoretischer und experimenteller Forschung gerückt.

Mit der in dieser Arbeit erfolgten erfolgreichen Demonstration von Destillation und Purifikation gequetschter Zustände ist der Weg geebnet für eine Demonstration analoger Protokolle für verschränkte Zustände im Regime kontinuierlicher Variablen. Viele der entwickelten und verfeinerten experimentellen Techniken dieser Arbeit können unmittelbar übertragen werden, wenn verschränkte Zustände verwendet werden. Dies sind vor allem die Erzeugung nichtklassischer Zustände durch OPAs, phasengeregelte Übertragung auf Strahlteilern, Nachbildung störungsbehafteter Übertragungskanäle und Homodyndetektion mit rechnergestützter Datenerfassung.

Die Umsetzung von Destillation verschränkter Zustände ist ein notwendiger und unumgänglicher Grundbaustein für einen *quantum repeater*, der jede technologische Realisierung einer Quantenkommunikation über realistische Distanzen überhaupt erst ermöglicht.

Ein entsprechend aufgebautes Protokoll für die Destillation verschränkter Zustände, das dem Vorbild der in dieser Arbeit beschriebenen Verfahren folgt, würde erstmals die Präparation destillierter verschränkter Zustände im Regime kontinuierlicher Variablen erlauben.

Weiterhin mögen die in dieser Arbeit beschriebenen Experimente als Beispiel dafür dienen, wie ein – zunächst als *einfache Strategie* erdachtes – Vorgehen erst im Verlauf experimenteller Bearbeitung seine ganzen Möglichkeiten offenbart.

ANHANG **A**

Python Sources

In diesem Anhang ist der Quellcode der verwendeten Software zusammengestellt. Beim Programmieren in `Python` ist die Verwendung von Einrückungen ein wesentliches Syntaxmerkmal (und dient nicht – wie in den meisten anderen Sprachen – lediglich zur Strukturierung des Codes). Die Einrückungen sind daher explizit hervorgehoben. Lange Zeilen sind umgebrochen (was genau durch das Fehlen eines Einrückungszeichens am Zeilenanfang erkennbar wird). In der Regel wird lediglich die Hauptroutine angegeben. Um ein funktionsfähiges Programm zu erhalten, muss diese explizit, zum Beispiel per

```
1 if (__name__=="__main__"):
  →import sys
  →import os
  →import random
  →from math import *
6
  →Main()
```

aufgerufen werden. Die zu importierenden Pakete können für unterschiedliche Routinen verschieden sein. Da der Quellcode praktisch als Pseudocode gelesen werden kann, wird die Funktion der einzelnen Routinen nur kurz benannt und nicht in aller Ausführlichkeit dokumentiert. Weitere Hinweise zur Funktion und zum Zusammenspiel der einzelnen Programme und Routinen findet man vor allem in Kapitel 6.

A.1 Vacuum

Die Routine wird auf ein Standardeingabefile angewendet. Ein solches besteht aus beliebigen Metainformationen (Header) mit einer Anzahl von Zeilen, die durch `headerlines` gegeben ist. An den Header schließt sich eine zweispaltige Zahlenreihe an, die die Messwerte von HD1 und HD2 repräsentiert. Diese Routine liefert einfach die Varianzen der beiden Spalten zurück. Die Bezeichnung rührt daher, dass mit dieser Routine die Varianz der Vakuumreferenz bestimmt wird, die für die folgenden Messungen als Normierungsfaktor dient.

Eingabe: Standardeingabefile
Ausgabe: Zwei Varianzen
Helper: Keine

```
def Main():

    # Parameter

    filename = './data/vac.lvm'
    headerlines = 22
    readlines = 1000000

    # Einlesen des datenfiles

    fh = open(filename,'r')
    lines = fh.readlines()
    fh.close()

    # Leere arrays fuer die Werte initialisieren

    col1 = []
    col2 = []

    linecount = 1

    # Formatieren der Werte

    for line in lines:
        if (linecount > headerlines and linecount <= readlines
        + headerlines):
```

```
        line = line.strip()
        line_values = line.split('↪')

        col1.append(float(line_values[0]))
        col2.append(float(line_values[1]))

        linecount = linecount + 1

    # Werte von einem konstanten Offset befreien

    mean_col1 = MeanValue(col1)
    mean_col2 = MeanValue(col2)

    for i in range(len(col1)):
        col1[i] = (col1[i] - mean_col1)
        col2[i] = (col2[i] - mean_col2)

    # Ausgeben der Varianzen

    print 'Varianz 1:   ' + str(Variance(col1))
    print 'Varianz 2:   ' + str(Variance(col2))
```

A.2 Postprocess

Die Routine `postprocess` beseitigt den Effekt des nichtlinearen Phasenganges des Antialiasing-Filters. Dazu werden die Zeitserien von Messwerten (Standardeingabefile) zunächst einer FFT unterzogen. Anschließend kann mit der inversen Phase des Filters multipliziert und zurück transformiert werden. Zusätzlich zum Eingabefile erwartet die Routine die Transferfunktion des Filters. Dabei wird die gemessene Transferfunktion für beliebige Frequenzwerte linear interpoliert.

Eingabe: Standardeingabefile, Zwei Transferfunktionen
Ausgabe: Modifiziertes Standardeingabefile
Helper: Keine

```
def Main():
    # Parameter und Konstanten

    pi = 3.1415
```

```
    samplefreq = 100000

    filename = './data/sqzsqz035.lvm'
    outfilename = './data/sqzsqz035tf.dat'

    phasereadlines = 202

    headerlines = 22
    readlines = 50000

    # Braucht die Transferfunktion des AA-Filters

    phasech1name = 'Ch1.TXT'
    phasech2name = 'Ch2.TXT'

    # Datenfile einlesenn

    FILE = open(filename,'r')
    lines = FILE.readlines()
    FILE.close()

    # Formatieren der Werte

    col1 = []
    col2 = []

    linecount = 1

    for line in lines:
        if (linecount > headerlines and linecount <= readlines
      + headerlines):
            line = line.strip()
            line_values = line.split('\t')

            col1.append(float(line_values[0])) # Channel 1
            col2.append(float(line_values[1])) # Channel 2

        linecount = linecount + 1

    # Einlesen der Transferfunktion
    # Kanal 1
    FILE = open(phasech1name,'r')
    linespha = FILE.readlines()
    FILE.close()
```

```
49  →phacol1 = []
    →phacol2 = []

    →linecount = 1

54  →for line in linespha:
    → →if (linecount <= phasereadlines):
    → → →line = line.strip()
    → → →line_values = line.split('→')
    → → →phacol1.append(float(line_values[0])) # Frequenz
59  → → →phacol2.append(float(line_values[2])) # Phase
    → →linecount = linecount +1

    →# Kanal 2
    →FILE = open(phasech2name,'r')
64  →linespha2 = FILE.readlines()
    →FILE.close()

    →phacol3 = []
    →phacol4 = []
69
    →linecount = 1

    →for line in linespha2:
    → →if (linecount <= phasereadlines):
74  → → →line = line.strip()
    → → →line_values = line.split('→')
    → → →phacol3.append(float(line_values[0])) # Frequenz
    → → →phacol4.append(float(line_values[2])) # Phase
    → →linecount = linecount +1
79
    →# In arrays umsetzen

    →phacol1array = array(phacol1)
    →phacol2array = array(phacol2)
84
    →phacol3array = array(phacol3)
    →phacol4array = array(phacol4)

    →# Kanal 1 korrigieren
89
    →# FFT durchfuehren
```

```
    →col1array = array(col1)
    →col2array = array(col2)
94
    →col1arrayfft = fft(col1array)
    →col2arrayfft = fft(col2array)

    →currentfreq = array([0])
99
    →maxlength = len(col1arrayfft)
    →halflength = maxlength/2

    →# for i in range(len(col1arrayfft)):
104 →for i in range(halflength):
    → →currentfreq[0] = i * float(samplefreq)/float(readlines)
    → →phasethere = arrayfns.interp(phacol2array,phacol1array,
      currentfreq)
    → →phasethere2 = arrayfns.interp(phacol4array,phacol3array
      ,currentfreq)
    → →# print phasethere
109 → →# print col1arrayfft[i]
    → →col1arrayfft[i] = col1arrayfft[i] * exp(-1j *
      phasethere[0] * 2.0 * pi /360.0)
    → →col1arrayfft[maxlength-1-i] = col1arrayfft[maxlength-1-
      i] * exp(1j * phasethere[0] * 2.0 * pi /360.0)
    → →col2arrayfft[i] = col2arrayfft[i] * exp(-1j *
      phasethere2[0] * 2.0 * pi /360.0)
    → →col2arrayfft[maxlength-1-i] = col2arrayfft[maxlength-1-
      i] * exp(1j * phasethere2[0] * 2.0 * pi /360.0)
114
    →# Zuruecktransformieren

    →backtransformed = ifft(col1arrayfft)
    →backtransformed2 = ifft(col2arrayfft)
119
    →# In ein file schreiben

    →FILE = open(outfilename,'w')
    →for i in range(len(backtransformed)):
124 → →FILE.write(str(real(backtransformed[i])) + '↪' + str(
      real(backtransformed2[i])) + '\n')
    →FILE.close()
```

A.3 Simulation

Erstellt Eingabefiles mit Werten, die gemessenen Datenreihen entsprechen. Dazu werden zunächst Reihen von Zufallszahlen erstellt, die Quadraturmesswerte repräsentieren. Diese werden dann mit zufälligem Phasenrauschen versehen und an einem Strahlteiler überlagert. Die sich ergebenden Messwerte in den beiden Ausgängen des Strahlteilers werden in eine Datei geschrieben, die genau wie gemessene Daten weiter verarbeitet werden können.

Eingabe: Eingabeparameter
Ausgabe: Standardeingabefile
Helper: MakeNoise

```
def Main():
    # Parameter der Purifikation

    outfilename = 'simutest2.lvm'

    modus = 1 # 1:sqzsqz, 2:sqzAsqz

    number_of_points = 100000

    opa1amp_value = 0.32
    opa1pha_value = 8.5
    opa2amp_value = 0.32
    opa2pha_value = 8.5

    sigma_of_noise = 0.4

    # Initialisieren der benoetigten arrays

    opa1amp = []
    opa1pha = []
    opa2amp = []
    opa2pha = []

    opa1ampnew=[]
    opa1phanew=[]
    opa2ampnew=[]
    opa2phanew=[]

    noise1 = []
```

```
30  →noise2 = []

    →port1amp = []
    →port1pha = []

35  →port2amp = []
    →port2pha = []

    →# Generieren der Startwerte
    →print 'Messwerte␣erstellen'
40  →for i in range(number_of_points):
    →  →# Generieren der Messwerte
    →  →opa1amp.append(float(random.gauss(0,opa1amp_value**0.5)
       ))
    →  →opa1pha.append(float(random.gauss(0,opa1pha_value**0.5)
       ))
    →  →opa2amp.append(float(random.gauss(0,opa2amp_value**0.5)
       ))
45  →  →opa2pha.append(float(random.gauss(0,opa2pha_value**0.5)
       ))

    →print 'Noise␣erstellen'

    →noise1 = MakeNoise(number_of_points)
50  →noise2 = MakeNoise(number_of_points)
    →noise1a = numpy.array(noise1)
    →noise2a = numpy.array(noise2)

    →varnoise1a = numpy.var(noise1a)
55  →varnoise2a = numpy.var(noise2a)

    →noise1a = noise1a / sqrt(varnoise1a) * sigma_of_noise
    →noise2a = noise2a / sqrt(varnoise2a) * sigma_of_noise

60  →print 'Messwerte␣verrauschen'
    →for i in range(number_of_points):
    →  →opa1ampnew.append(opa1amp[i] * cos(noise1a[i]) +
       opa1pha[i] * sin(noise1a[i]))
    →  →opa1phanew.append(opa1pha[i] * cos(noise1a[i]) -
       opa1amp[i] * sin(noise1a[i]))
    →  →opa2ampnew.append(opa2amp[i] * cos(noise2a[i]) +
       opa2pha[i] * sin(noise2a[i]))
65  →  →opa2phanew.append(opa2pha[i] * cos(noise2a[i]) -
       opa2amp[i] * sin(noise2a[i]))
```

```
    →opa1amp = opa1ampnew
    →opa1pha = opa1phanew
    →opa2amp = opa2ampnew
70  →opa2pha = opa2phanew

    →# Verlustkanal

    →# opa1amp = MakeLoss(opa1amp,35.0)
75  →# opa1pha = MakeLoss(opa1pha,35.0)
    →# opa2amp = MakeLoss(opa2amp,35.0)
    →# opa2pha = MakeLoss(opa2pha,35.0)

    →print 'Purifikations-Strahlteiler'
80  →for i in range(number_of_points):
    → →port1amp.append((opa1amp[i] + opa2amp[i])*(1/(2**0.5)))
    → →port1pha.append((opa1pha[i] + opa2pha[i])*(1/(2**0.5)))
    → →port2amp.append((opa1amp[i] - opa2amp[i])*(1/(2**0.5)))
    → →port2pha.append((opa1pha[i] - opa2pha[i])*(1/(2**0.5)))
85
    →# Schreiben des datenfiles
    →FILE = open(outfilename,'w')
    →if modus == 1:
    → →for d in range(number_of_points):
90  → → →FILE.write(str(port1amp[d])+'→'+str(port2amp[d])+'\n
      ')
    →if modus == 2:
    → →for d in range(number_of_points):
    → → →FILE.write(str(port1amp[d])+'→'+str(port2pha[d])+'\n
      ')

95  →FILE.close()
```

A.4 Purify

Diese Routine erledigt das eigentliche Destillationsprotokoll. Dazu wird ein Standardeingabefile geladen. Anschließend wird für einen gewählten Schwellenwert Q die Konditionierungsbedingung geprüft. Von allen Messwerten, die der Konditionierungsbedingung genügen wird abschließend die Varianz berechnet. Die drei Ausgabewerte *Schwellenwert*, *Erfolgswahrscheinlichkeit* und

Ausgabevarianz werden in eine Datei geschrieben. Mittels einer Schleife wird dieser Zyklus für mehrere Schwellenwerte Q wiederholt.

Eingabe: Standardeingabefile
Ausgabe: Ausgabefile mit Q, P und V_{out}
Helper: Postprocess

```
def Main():
    # Parameter der Purifikation

    filename = 'simutest2.lvm'
    outfilename = 'purplotnum2.dat'
    headerlines = 22
    readlines = 80000
    resolution_points = 20
    max_trigger = 5.0
    min_trigger = 0.1
    vacuum1_variance = 1.0
    vacuum2_variance = 1.0

    intervall = max_trigger/resolution_points

    # Einlesen des datenfiles
    fh = open(filename,'r')
    lines = fh.readlines()
    fh.close()

    # Leere arrays fuer die Werte initialisieren
    col1 = []
    col2 = []

    linecount = 1

    # Formatieren der Werte
    for line in lines:
        if (linecount > headerlines and linecount <= readlines
        + headerlines):
            line = line.strip()
            line_values = line.split('\t')

            col1.append(float(line_values[0]))
            col2.append(float(line_values[1]))

```

```
→ →linecount = linecount + 1

→# Werte in ein numpy array schreiben

→col1array = array(col1)
→col2array = array(col2)

→# Werte von einem konstanten Offset befreien
→# und auf das Vakuumrauschen normieren

→col1array = (col1array - col1array.mean())/sqrt(
  vacuum1_variance)
→col2array = (col2array - col2array.mean())/sqrt(
  vacuum2_variance)

→# File zum Schreiben oeffnen und die Purifikation
  durchfuehren
→FILE = open(outfilename,'w')
→for d in range(resolution_points):
→ →# purifiziert = PostSelect(col1, col2, (intervall * d +
   min_trigger))
→ →# FILE.write(str(intervall * d + min_trigger) + ' ' +
  str(Variance(purifiziert)) + '\n') # Ueber Trigger
→ →# FILE.write(str(float(len(purifiziert))/float(len(col1
  ))) + ' ' + str(Variance(purifiziert)) + '\n') # Ueber FOS
→ →purifiziert = PostSelectNumpy(col1array, col2array, (
  intervall * d + min_trigger))
→ →FILE.write(str(intervall * d + min_trigger) + '␣' + str
  ((float(purifiziert.size))/(float(col1array.size))) + '␣'
  + str(var(purifiziert)) + '\n')
→FILE.close()
```

A.5 Helpers

A.5.1 Powerspectrum

Erhält ein Standardeingabefile und liefert als Ausgabe ein Leistungsspektrum entweder der ersten oder der zweiten Spalte.

Eingabe: Standardeingabefile
Ausgabe: Datei mit Leistungsspektrum
Helper: Keine

```
def Main():
    filename = './data/sqzsqz035.lvm'
    outfilename = './data/powerspectrum3.dat'
    samplefreq = 100000

    headerlines = 22
    readlines = 30000

    # Datenfile einlesenn

    fh = open(filename,'r')
    lines = fh.readlines()
    fh.close()

    # Leere arrays fuer die Werte initialisieren
    col1 = []
    col2 = []

    linecount = 1

    # Formatieren der Werte
    for line in lines:
        if (linecount > headerlines and linecount <= readlines
        + headerlines):
            line = line.strip()
            line_values = line.split('\t')

            col1.append(float(line_values[0]))
            col2.append(float(line_values[1]))

        linecount = linecount + 1
```

```
    →# Werte in ein numpy array schreiben
33
    →col1array = array(col1)
    →col2array = array(col2)

    →# Jetzt ein Powerspectrum gewinnen
38
    →col1fft = fft(col2array)
    →powerspec = abs(col1fft * conjugate(col1fft))/len(
      col1array)**2

    →# In ein file schreiben
43
    →FILE = open(outfilename,'w')
    →for i in range(readlines/2):
    → →FILE.write(str(float(i * samplefreq / readlines)) + '␣'
      +str(powerspec[i]) + '\n')

48  →FILE.close()
```

A.5.2 MakeNoise

Erstellt das zufällige Phasenrauschen für die Simulation. Dazu werden zunächst Zufallszahlen erzeugt, die eine gaußförmige Verteilung haben. Diese werden anschließend mit einem digitalen Filter auf das Frequenzband zwischen 1 kHz und 5 kHz eingeschränkt. Um das Einschwingverhalten des Filters zu berücksichtigen, werden mehr Werte produziert als letztendlich benötigt. der Teil des Datenstroms, der vom Einschwingverhalten beeinträchtigt wird, wird vor Anwendung des Rauschens entfernt.

Eingabe: Eingabeparameter
Ausgabe: Liefert gefiltertes Rauschen zurück
Helper: Keine

```
def MakeNoise(points):
2   →SafetyMargin = 50000 # Einschwingverhalten

    →# Zunächst Rauschen erstellen
    →x = []
    →y = []
7   →z = []
```

```
    →for i in range(points + SafetyMargin):
    →  →x.append(0.0)
    →  →y.append(0.0)
    →  →#z.append(0.0)

    →for i in range(points + SafetyMargin):
    →  →#x.append(random.gauss(0,1))
    →  →#y.append(0.0)
    →  →x[i] = random.gauss(0,1)

    →# Filter anwenden

    →a0 =0.00045921618388999088
    →a1 =0.0
    →a2 =-0.0018368647355599635
    →a3 =0.0
    →a4 =0.0027552971033399454
    →a5 =0.0
    →a6 =-0.0018368647355599635
    →a7 =0.0
    →a8 =0.00045921618388999088
    →b0 =1.00
    →b1 =-7.1732007945
    →b2 =22.6385602238
    →b3 =-41.0695071546
    →b4 =46.8533814786
    →b5 =-34.4255969981
    →b6 =15.9105081693
    →b7 =-4.2291670230
    →b8 =0.4950222052

    →for n in range(points + SafetyMargin):
    →  →y[n] = a0 * x[n-0] + a2 * x[n-2] + a4 * x[n-4] + a6*x[n
       -6] + a8 * x[n-8] - b1*y[n-1] - b2*y[n-2]- b3*y[n-3]- b4*y
       [n-4]- b5*y[n-5]- b6*y[n-6]- b7*y[n-7]- b8*y[n-8]

    →# Den SafetyMargin wegwerfen

    →for i in range(points):
    →  →z.append(y[i+SafetyMargin])

    →return z
```

A.5.3 MakeLoss

Diese Routine kann im Rahmen einer Simulation verwendet werden, um an einer beliebigen Stelle einen optischen Verlust einzuführen. Dazu wird ein Strahlteiler mit einem offenen Eingang, durch den Vakuumrauschen einkoppelt, simuliert.

Eingabe: Eingabeparameter, Array von Messwerten
Ausgabe: Liefert modifiziertes Array zurück
Helper: Keine

```
def MakeLoss(data, loss):
    # Data ist ein Messwertfile, loss ein Verlust in Prozent
    # Es wird ein Strahlteiler simuliert, der ein Vakuum
      beimischt

    print 'Applying Loss of ' +str(loss)+' %'

    vacuum = []
    after_loss = []

    transmittivity = 1 - (loss/100)
    reflectivity = 1 - transmittivity

    number_of_points = len(data)

    for i in range(number_of_points):
        vacuum.append(float(random.gauss(0,1)))

    for i in range(number_of_points):
        after_loss.append((sqrt(transmittivity) * data[i]) + (
      sqrt(reflectivity) * vacuum[i]))

    return after_loss
```

A.5.4 PostSelect

Die `postselect` Routinen erledigen die Prüfung von simulierten oder gemessenen Daten bezüglich der Erfüllung der Konditionierungsbedingung. `postselect` führt dabei eine einfache Purifikation durch, während eine nachgestellte Ziffer X darauf hinweist, dass zusätzlich *quantum channel probing* mit $N_{\mathrm{QCP}} = X$ durchgeführt wird.

Eingabe: Zwei Arrays mit Messwerten, Schwellenwert
Ausgabe: Array mit selektierten Messwerten
Helper: Keine

```
def PostSelectNumpy(c1, c2, trigger):
  →print 'Postselecting␣with␣trigger␣' + str(trigger)

4 →c2 = abs(c2)
  →condition = (c2 < trigger)

  →return c1.compress(condition)
```

A.5.5 PostSelect2

```
def PostSelectNumpy2(c1, c2, trigger):
  →print 'Postselecting␣with␣trigger␣' + str(trigger)
3
  →c2 = abs(c2)

  →selected = []

8 →for i in range(c2.size):
  → →if (i>0):
  → → →trig = c2[i]
  → → →trig2 = c2[i-1]

13 → → →if (trig<trigger and trig2<trigger):
  → → → →selected.append(c1[i])

  →postsel = array(selected)
  →return postsel
```

A.5.6 PostSelect4

```
def PostSelectNumpy4(c1, c2, trigger):
 →print 'Postselecting␣with␣trigger␣' + str(trigger)

 →c2 = abs(c2)

 →selected = []

 →for i in range(c2.size):
 → →if (i>2):
 → → →trig = c2[i]
 → → →trig2 = c2[i-1]
 → → →trig3 = c2[i-2]
 → → →trig4 = c2[i-3]

 → → →if (trig<trigger and trig2<trigger and trig3<trigger
    and trig4<trigger):
 → → → →selected.append(c1[i])

 →postsel = array(selected)
 →return postsel
```

ANHANG **B**

Felder und Strahlteiler

B.1 Strahlteilermatrix

Von besonderer Wichtigkeit für die hier beschriebene Arbeit ist die Wirkungsweise von Strahlteilern auf optische Felder. Als Purifikationsstrahlteiler (Kapitel 4) ist ein Strahlteiler ein essentieller Bestandteil des beschriebenen Protokolls zur Destillation und Purifikation von gequetschten Zuständen. Auch Homodyndetektion als Detektionsverfahren der Wahl basiert im Wesentlichen auf den besonderen Eigenschaften eines Strahlteilers. Wir beschreiben die Wirkungsweise von einem Strahlteiler auf Felder also im Folgenden vergleichsweise ausführlich. Dabei verfolgen wir einen abstrakten Ansatz. Demnach betrachten wir einen Strahlteiler als eine „Maschine“, welche zwei Eingangsfelder α_i in zwei Ausgangsfelder β_i transformiert. Der Effekt eines solchen Strahlteilers kann durch eine Matrix $\mathbf{S}$ mit vorerst unbekannten Einträgen repräsentiert werden:

$$\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} = \mathbf{S}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}. \tag{B.1}$$

Als Annahme führt man nun ein, dass dieser Prozess reversibel sein soll, also unter Zeitumkehr in gleicher Weise stattfindet. Man beachte, dass unter Zeitumkehr die Felder komplex konjugiert werden müssen:

$$\begin{pmatrix}\alpha_1^*\\ \alpha_2^*\end{pmatrix} = \mathbf{S}\begin{pmatrix}\beta_2^*\\ \beta_1^*\end{pmatrix}. \tag{B.2}$$

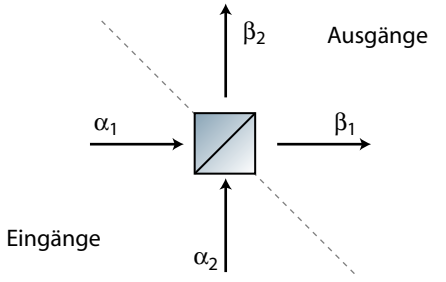

Abbildung B.1 — Ein abstraktes Strahlteilermodell. Wir betrachten einen Strahlteiler als „Maschine“, die die beiden Eingangsfelder α_1 und α_2 in die beiden Ausgangsfelder β_1 und β_2 transformiert.

Man beachte außerdem, dass in dieser Gleichung die Indizes an den Ausgangsfeldern vertauscht erscheinen. Dies folgt aus der Geometrie und wird einsehbar, wenn man die Felder in der ⇝Abbildung B.1 durch *Rotation* entsprechend umordnet. Die Reihenfolge der Indizes kann wiederum zurück vertauscht werden, wenn man die Matrix transponiert, denn dadurch vertauschen gerade die Eingangsfelder ihre Rollen.

$$\begin{pmatrix} \alpha_1^* \\ \alpha_2^* \end{pmatrix} = \mathbf{S}^T \begin{pmatrix} \beta_1^* \\ \beta_2^* \end{pmatrix}. \tag{B.3}$$

Um besser mit (⇝Gleichung (B.1)) vergleichen zu können, multipliziert man auf beiden Seiten mit der inversen Matrix:

$$\begin{pmatrix} \beta_1^* \\ \beta_2^* \end{pmatrix} = \mathbf{S}^{T^{-1}} \begin{pmatrix} \alpha_1^* \\ \alpha_2^* \end{pmatrix}. \tag{B.4}$$

Indem man auf beiden Seiten komplex konjugiert, erhält man:

$$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \mathbf{S}^{T^{-1^*}} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}. \tag{B.5}$$

Durch Vergleich mit (⇝Gleichung (B.1)) sieht man

$$\mathbf{S} = \mathbf{S}^{T^{-1^*}} \Leftrightarrow \mathbf{S} = \mathbf{S}^{\dagger^{-1}} \Leftrightarrow \mathbf{S}^\dagger \mathbf{S} = 1, \tag{B.6}$$

wobei die letzte Gleichung die Unitarität von **S** bedeutet. Diese letzte Gleichung kann man ausführlich aufschreiben, um die einzelnen Komponenten von **S** zu gewinnen:

$$\mathbf{S}^\dagger\mathbf{S} = \begin{pmatrix} A^* & C^* \\ B^* & D^* \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{B.7}$$

Wertet man diese Gleichung zeilenweise aus, findet man:

$$\left.\begin{array}{l} A^*A + C^*C = 1 \\ B^*A + D^*C = 0 \\ B^*B + D^*D = 1 \\ A^*B + C^*D = 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} A^*A = D^*D \\ B^*B = C^*C \end{array}\right\} \Rightarrow \begin{array}{l} |A| = |D| = \rho \\ |B| = |C| = \tau \end{array}. \tag{B.8}$$

Damit liegen jedoch zunächst nur die Absolutbeträge der Matrixelemente fest. Es können noch beliebig Phasenfaktoren vorliegen. Startet man wieder mit ⇝Gleichung (B.7), kann man aufschreiben:

$$\mathbf{S}^\dagger\mathbf{S} = \begin{pmatrix} \rho\exp(-i\phi_1) & \tau\exp(-i\phi_3) \\ \tau\exp(-i\phi_2) & \rho\exp(-i\phi_4) \end{pmatrix}\begin{pmatrix} \rho\exp(i\phi_1) & \tau\exp(i\phi_2) \\ \tau\exp(i\phi_3) & \rho\exp(i\phi_4) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{B.9}$$

Wiederum kann man diese Gleichung zeilenweise auswerten und findet zum einen

$$\rho^2 + \tau^2 = 1 \tag{B.10}$$

und zum anderen

$$\exp(i(\phi_2 - \phi_1)) + \exp(i(\phi_4 - \phi_3)) = 0. \tag{B.11}$$

Aus der letzten Gleichung liest man eine wichtige Beziehung zwischen den einzelnen Phasentermen am Strahlteiler ab. Es folgt nämlich:

$$(\phi_2 - \phi_1) - (\phi_4 - \phi_3) = \pm(2n-1)\pi \tag{B.12}$$

B.2 Die Unitarität der Strahlteilermatrix

Die Unitarität der Strahlteilermatrix kann man auch unmittelbarer einsehen, wenn man verlangt, dass bei den Transformationen die Energie erhalten ist (eine Voraussetzung für die Reziprozität).

$$P_{\text{out}} = \langle b|\, b\rangle = \langle \mathbf{S}a|\, \mathbf{S}a\rangle = \langle a|\, \mathbf{S}^\dagger\mathbf{S}\,|a\rangle = P_{\text{in}}. \tag{B.13}$$

Verlangt man nun aus Gründen der Energieerhaltung, dass $P_{\text{out}} = P_{\text{in}}$ sein soll, so gilt dies genau dann wenn $\mathbf{S}^{\dagger}\mathbf{S} = 1$, womit die Unitarität der Strahlteilermatrix festgesetzt ist.

B.3 Symmetrischer Fall

Wir betrachten einen völlig symmetrischen Strahlteiler. In diesem Fall gibt es keinen Grund zu der Annahme, dass etwa die beiden Reflektionen unterschiedliche Phasen erhalten sollten. Wir wählen also diese beiden Phasen zu Null:

$$\phi_1 = \phi_4 = 0. \tag{B.14}$$

Aus der Beziehung zwischen den Phasen folgt dann, dass $\phi_2 + \phi_3 = \pi$. Man kann also wählen:

$$\phi_2 = \phi_3 = \frac{\pi}{2}. \tag{B.15}$$

Damit liegen alle Phasenterme fest und wir können für die Strahlteilermatrix des symmetrischen Strahlteilers aufschreiben:

$$\mathbf{S} = \begin{pmatrix} \rho & i\tau \\ i\tau & \rho \end{pmatrix}, \tag{B.16}$$

wobei ρ und τ die Reflektivität und die Transmission für die Felder bezeichnet.

B.4 Unsymmetrischer Fall

Im unsymmetrischen Fall erhält man etwa für die erste Reflektion einen Phasensprung von $\phi_4 = \pi$. Damit können die übrigen Phasen alle zu Null gewählt werden:

$$\phi_1 = \phi_2 = \phi_3 = 0. \tag{B.17}$$

Somit kann man als Matrix für den unsymmetrischen Strahlteiler angeben:

$$\mathbf{S} = \begin{pmatrix} \rho & \tau \\ \tau & -\rho \end{pmatrix}. \tag{B.18}$$

Literaturverzeichnis

[And04] U. L. Andersen, O. Glöckl, S. Lorenz, G. Leuchs, R. Filip, „*Experimental Demonstration of Continuous Variable Quantum Erasing*“, Phys. Rev. Lett. **93**, 100403 (2004).

[Bac04] H.-A. Bachor, T. Ralph, „*A Guide to Experiments in Quantum Optics*“, WILEY-VCH Verlag GmbH, Weinheim (2004).

[Ben84] C. H. Bennett, G. Brassard, „*Quantum Cryptography: Public Key Distribution and Coin Tossing*“, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India (1984).

[Ben92] C. H. Bennett, S. J. Wisner, „*Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*“, Phys. Rev. Lett. **69**, 2881 (1992).

[Ben96] C. H. Bennett, G. Brassard, S. Popescue, B. Schumacher, J. A. Smolin, W. Wootters, „*Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*“, Phys. Rev. Lett. **76**, 722 (1996).

[Bla00] E. D. Black, „*An introduction to Pound-Drever-Hall laser frequency stabilization*“, Am. J. Phys. **69**, 79 (2000).

[Bra05] S. L. Braunstein, P. van Loock, „*Quantum information with continuous variables*“, Rev. Mod. Phys. **77**, 513 (2005).

[Bro03] D. E. Browne, J. Eisert, S. Scheel, M. Plenio, „*Driving non-Gaussian to Gaussian states with linear optics*“ Phys. Rev. A **67**, 062320 (2003).

[Bru07] D. Bruß, G. Leuchs (Editoren), „*Lectures on Quantum Information*“, WILEY-VCH Verlag GmbH, Weinheim (2007).

[Cav81] C. M. Caves, „*Quantum-mechanical noise in an interferometer*“, Phys. Rev. D **23**, 1693 (1981).

[Dar27] C. G. Darwin, „*Free motion in wave mechanics*“, Proc. Camb. Phil. Soc. **117**, 258 (1927).

[Deu96] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescue, A. Sanpera, „*Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*“, Phys. Rev. Lett. **77**, 2818 (1996).

[Dod02] V. V. Dodonov, „*'Nonclassical' states in quantum optics: a 'squeezed' review of the first 75 years*“, J. Opt. B:Quantum Semiclass. Opt. **4**, R1 (2002).

[Eis02] J. Eisert, S. Scheel, M. B. Plenio, „*Distilling Gaussian States with Gaussian Operations is Impossible*“, Phys. Rev. Lett. **89**, 137903 (2002).

[Eis04] J. Eisert, D. E. Browne, S. Scheel, M. B. Plenio, „*Distillation of continuous-variable entanglement with optical means*“ Ann. Phys. **311** 431 (2004).

[Fiu02] J. Fiurášek, „*Gaussian Transformations and Distillation of Entangled Gaussian States*“, Phys. Rev. Lett. **89**, 137904 (2002).

[Fra03] A. Franzen, „*Erzeugung von gequetschtem Licht für die Gravitationswellenastronomie*“, Diplomarbeit Universität Hannover (2003).

[Fra06] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, R. Schnabel, „*Experimental Demonstration of Continuous Variable Purification of Squeezed States*“, Phys. Rev. Lett. **97**, 150505 (2006).

[Fur98] A. Furusawa, J. L. Sørensen, S. L- Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, „*Unconditional Quantum Teleportation*“, Science **282**, 706 (1998).

[Ger05] C. Gerry, P. Knight, „*Introductory Quantum Optics*“, Cambridge University Press (2005).

[Gie02] G. Giedke, J. I. Cirac, „*Characterization of Gaussian operations and distillation of Gaussian states*“, Phys. Rev. A **66**, 032316 (2002).

[Gis02] N. Gisin, G. Ribordy, W. Tittel, H. binden, „*Quantum cryptography*“, Rev. Mod. Phys. **74**, 145 (2002).

[Gro03] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, P. Grangier, „*Quantum key distribution using gaussian-modulated coherent states*“, Nature **421**, 238 (2003).

[Hag07] B. Hage, A. Franzen, J. DiGuglielmo, P. Marek, J. Fiurášek, R. Schnabel, „*On the distillation and purification of phase-diffused squeezed states*“, New Journal of Physics **9**, 227 (2007).

[Hir03] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, R. Namiki, „*Quantum cryptography using pulsed homodyne detection*“, Phys. Rev. A **68**, 042331 (2003).

[Hol79] J. N. Hollenhorst, „*Quantum limits on resonant-mass gravitational-radiation detectors*“, Phys. Rev. D **19**, 1669 (1979).

[Jia04] X. Jia, X. Su, Q. Pan, J. Gao, C. Xie, K. Peng, „*Experimental Demonstration of Unconditional Entanglement Swapping for Continuous Variables*“, Phys. Rev. Lett. **93**, 250503 (2004).

[Ken27] E. H. Kennard, „*Zur Quantenmechanik einfacher Bewegungstypen*“, Z. Phys. **44**, 326 (1927).

[Knu81] D. E. Knuth, „*The Art of Computer Programming*“, 2. Auflage, Addison-Wesley (1981).

[Kra03] B. Kraus, K. Hammerer, G. Giedke, J. I. Cirac, „*Entanglement generation and Hamiltonian simulation in continuous-variable systems*“, Phys. Rev. A **67**, 042314 (2003).

[Kwi01] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, N. Gisin „*Experimental entanglement distillation and 'hidden' non-locality*“ Nature **409**, 1014 (2001).

[Lan04] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, P. K. Lam, „*Tripartite Quantum State Sharing*“ Phys. Rev. Lett. **92**, 177903 (2004).

[Leh51] D. H. Lehmer, „*Mathematical methods in large-scale computing units*“, Annu. Comput. Lab. Harvard Univ. 26, 141 (1951).

[Mar07] P. Marek, J. Fiurášek, B. Hage, A. Franzen, J. DiGuglielmo, R. Schnabel, „*Iterative distillation and purification of phase diffused squeezed states*“, Phys. Rev. A **67**, 053820 (2007).

[Mon95] C. Monroe, D. .M. Meekhof, B. E. King, W. M. Itano, D. J. Wineland, „*Demonstration of a Fundamental Quantum Logic Gate*“, Phys. Rev. Lett. **75**, 4714 (1995).

[Par88] S. K. Park, K. W. Miller, „*Random Number Generators: Good Ones Are Hard To Find*“, Commun. ACM 31(10): 1192 (1988).

[Sch26] E. Schrödinger, „*Der stetige Übergang von der Mikro- zur Makromechnik*“, Naturwissenschaften **14**, 664 (1926).

[Sha48] C. E. Shannon, „*A Mathematical Theory of Communication*“, Bell System Technical Journal, 27, 379 and 623 (1948).

[Pan01] J.-W. Pan, C. Simon, C. Brukner, A. Zeilinger, „*Entanglement purification for quantum communication*“, Nature **410**, 1067 (2001).

[Pan03] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, A. Zeilinger, „*Experimental entanglement purification of arbitrary unknown states*“, Nature **423**, 417 (2003).

[Slu85] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, J. F. Valley, „*Observation of Squeezed States Generated by Four-Wave Mixing in an Optical Cavity*“, Phys. Rev. Lett. **55**, 2409 (1985).

[Wig32] E. P. Wigner, „*On the quantum correction for thermodynamic equilibrium*“, Phys. Rev. **40**, 749—759 (1932).

[Yam03] T. Yamamoto, M. Koashi, S. Özdemir, N. Imoto, „*Experimental extraction of an entangled photon pair from two identically decohered pairs*“, Nature **421**, 343 (2003).

[Yue76] H. P. Yuen, „*Two photon coherent state of the radiation field*“, Phys. Rev. A 13, 2226 (1976) .

Danksagung

Am Zustandekommen dieser Doktorarbeit war über die Jahre eine Vielzahl von Personen – auf die eine oder andere Weise – beteiligt.

Zunächst schulde ich Herrn Prof. Dr. Karsten Danzmann vielfachen Dank. Er hat am Max-Planck-Institut für Gravitationsphysik diese Arbeit mit Grundlage und Substanz versehen und damit überhaupt erst ermöglicht.

Gleichsam vielfachen Dank schulde ich Herrn Jun.-Prof. Dr. Roman Schnabel, der diese Arbeit auf den Weg gebracht hat und durch stetige Betreuung, Hilfsbereitschaft, hervorragende Ideen und motivierende Impulse[1] an Mühe und Erfolg persönlichen Anteil genommen hat.

Großen Dank bringe ich auch Herrn Dr. Jaromir Fiurášek entgegen, der mit seinen präzisen Vorstellungen über Destillation und Purifikation von Quantenzuständen dem experimentellen Vorhaben hinter der vorliegenden Arbeit mehr als nur den Startschuss lieferte.

Eigentlich an erster Stelle zu nennen, danke ich meiner Familie, allen voran meiner Frau Mirjam. Ihre liebevolle Unterstützung war ein stetiger Rückenwind auf diesem Weg. Samuel und Emily May waren mir Lohn für so manche Mühe und *zwei gute Gründe.* Meinen Eltern danke ich für Jahrzehnte der Unterstützung und Treue . . . weit über das Maß des Notwendigen hinaus.

Besonderer Dank geht an die Mitglieder meiner Arbeitsgruppe, die nicht nur mit manch guter Idee den Erfolg dieser Arbeit mitgetragen haben, sondern vor allem ein freundschaftliches und lebensnahes Arbeitsklima geschaffen haben, in dem Kreativität überhaupt erst möglich war. Hier sind zu nennen: Herr Dipl.-Phys. Boris Hage, ohne den diese Arbeit um ihre Existenz ärmer wäre, Herr Dipl.-Phys. Henning Vahlbruch, Herr Dr. Simon Chelkowski, Herr Dipl.-Phys. James DiGuglielmo, Herr Dipl.-Phys. Andre Thüring, Herr Dipl.-Phys. Nico Lastzka, Herr Dipl.-Phys. Moritz Mehmet und Herr Dr. Stefan Gossler.

[1] Auch bekannt als: Feuer unterm Hintern.

Hunderte von Fehlern im Manuskript dieser Arbeit wurden zuverlässig aufgespürt durch die geduldige und sorgfältige Arbeit von: Herrn Leonhard Franzen, Herrn Dr. Stefan Gossler, Herrn Dipl.-Phys. Andre Thüring, Herrn Dipl.-Phys. Aiko Samblowski, Herrn Dipl.-Phys. Boris Hage, Herrn Dipl.-Phys. Daniel Friedrich, Herrn Dipl.-Phys. Henning Vahlbruch, Frau Mirjam Franzen, Herrn Dipl.-Phys. James DiGuglielmo, Herrn Dipl.-Phys. Moritz Mehmet, Herrn Dipl.-Phys. Malte Priest und Herrn Dipl.-Phys. Oliver Burmeister. Für verbleibende Fehler bin alleine ich verantwortlich. Wer nach Drucklegung noch einen findet – darf ihn behalten.

Alexander Franzen, Dezember 2007

Lebenslauf

Persönliche Daten »	Name: Alexander Franzen Geburtsdatum: 25. Mai 1977 Geburtsort: Würzburg Familienstand: verheiratet mit Mirjam Franzen Kinder: Samuel Josef, Emily May
Schulische Ausbildung »	1996: Abitur am Hölty-Gymnasium in Wunstorf (Leistungsfächer: Physik/Mathematik)
Wehrdienst »	1996–1997: Zivildienst bei der Arbeiterwohlfahrt Hildesheim
Studium »	1997– 2004: Physik-Studium an der Leibniz Universität Hannover 2003/2004: Diplomarbeit am Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) in Hannover 2004: Diplom in Physik ab Feb. 2004: Promotion am Max-Planck-Institut für Gravitationsphysik in Hannover

Eigene Veröffentlichungen

— 2003 —

1 | J. Harms, Y. Chen, S. Chelkowski, A. Franzen, H. Vahlbruch, K. Danzmann, and R. Schnabel, „*Squeezed-input, optical-spring, signal-recycled gravitational-wave detectors*“, Phys. Rev. A **67**, 012316 (2003).

2 | A. Franzen, „*Erzeugung von gequetschtem Licht für die Gravitationswellenastronomie*“, Diplomarbeit Universität Hannover (2003).

— 2004 —

3 | R. Schnabel, H. Vahlbruch, A. Franzen, S. Chelkowski, N. Grosse, H.-A. Bachor, W. P. Bowen, P. K. Lam, and K. Danzmann, „*Squeezed light at sideband frequencies below* 100 *kHz from a single OPA*“, Opt. Commun. 240, 185–190 (2004).

— 2005 —

4 | S. Chelkowski, H. Vahlbruch, B. Hage, A. Franzen, N. Lastzka, K. Danzmann, and R. Schnabel, „*Experimental characterization of frequency-dependent squeezed light*“, Phys. Rev. A **71**, 013806 (2005).

5 | H. Grote, B. Allen, . . . , A. Franzen, . . . , I. Zawischa, „*The status of GEO600*“, Class. Quantum Grav. **22**, S193–S198 (2005).

6 | H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, and R. Schnabel, „*Demonstration of a squeezed-light-enhanced power- and signal-recycled Michelson interferometer*“, Phys. Rev. Lett. **95**, 211102 (2005).

— 2006 —

7 | H. Lück, M. Hewitson, . . . , A. Franzen, . . . , R. Zhu, „*Status of the GEO600 detector*“, Class. Quantum Grav. **23**, S71–S78 (2006).

8 | B. Willke, P. Ajith, . . . , A. Franzen, . . . , R. Zhu, „*The GEO-HF project*“, Class. Quantum Grav. **23**, S207–S214 (2006).

9 | H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, R. Schnabel, „*Squeezed-field injection for gravitational wave interferometers*“, Class. Quantum Grav. **23**, S251 - S257 (2006).

10 | H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, R. Schnabel, „*Coherent Control of Vacuum Squeezing in the Gravitational-Wave Detection Band*“, Phys. Rev. Lett. **97**, 011101 (2006).

11 | A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, and R. Schnabel, „*Experimental Demonstration of Continuous Variable Purification of Squeezed States*“, Phys. Rev. Lett. **97**, 150505 (2006).

— 2007 —

12 | B. Hage, A. Franzen, J. DiGuglielmo, P. Marek, J. Fiurášek, and R. Schnabel, „*On the distillation and purification of phase-diffused squeezed states*“, New Journal of Physics **9**, 227 (2007).

13 | J. DiGuglielmo, B. Hage, A. Franzen, J. Fiurášek, and R. Schnabel, „*Experimental characterization of Gaussian quantum-communication channels*“, Phys. Rev. A **76**, 012323 (2007).

14 | P. Marek, J. Fiurášek,B. Hage, A. Franzen, J. DiGuglielmo, R. Schnabel, „*Iterative distillation and purification pf phase diffused squeezed states*“, Phys. Rev. A **76**, 053820 (2007).

Index