VERIFYING OPTICAL ENTANGLEMENT

by

MEGAN R. RAY

A DISSERTATION

Presented to the Department of Physics
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

September 2013

DISSERTATION APPROVAL PAGE

Student: Megan R. Ray

Title: Verifying Optical Entanglement

This dissertation has been accepted and approved in partial fulfillment of the requirements for the Doctor of Philosophy degree in the Department of Physics by:

Michael G. Raymer	Chair
Steven J. van Enk	Advisor
Graham D. Kribs	Core Member
Jeffrey A. Cina	Institutional Representative

and

Kimberly Andrews Espy	Vice President for Research & Innovation/ Dean of the Graduate School

Original approval signatures are on file with the University of Oregon Graduate School.

Degree awarded September 2013

© 2013 Megan R. Ray

DISSERTATION ABSTRACT

Megan R. Ray

Doctor of Philosophy

Department of Physics

September 2013

Title: Verifying Optical Entanglement

We look at the problem of verifying optical entanglement for two types of states relevant to quantum information processing. One type occurs in Hong-Ou-Mandel interference and is relevant to quantum computing. The other type is time-frequency entanglement which is useful for quantum key distribution. For these types of states the conventional methods of entanglement verification do not work well, and we develop new criteria and methods to verify entanglement of such states. Explicitly, one method takes into account the possible multimode character of two photons, while the other method takes into account the missing data that occur due to the finite range of detectors.

This dissertation includes previously published and unpublished co-authored material.

CURRICULUM VITAE

NAME OF AUTHOR: Megan R. Ray

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:
University of Oregon, Eugene, Oregon

DEGREES AWARDED:
Doctor of Philosophy, Physics, 2013, University of Oregon
Master of Science, Physics, 2009, University of Oregon
Bachelor of Science, Physics and Mathematics, 2007, University of Oregon

GRANTS, AWARDS AND HONORS:
National Science Foundation GK-12 Fellowship

PUBLICATIONS:
Megan R. Ray & S. J. van Enk *Missing data outside the detector range (II): application to time-frequency entanglement* Submitted for publication in Physical Review A

Megan R. Ray & S. J. van Enk *Missing data outside the detector range: continuous variable entanglement verification and quantum cryptography* Accepted for publication in Physical Review A

Megan R. Ray & S. J. van Enk *Verifying entanglement in the Hong-Ou-Mandel dip*, Physical Review A **83**, 042318 (2011).

ACKNOWLEDGEMENTS

I owe thanks to many people that have made this possible.

First, to my advisor Steven, as well as my lab mates Jun and Lucia, and the Raymer and Steck groups.

To my parents for their unconditional love and support and everything they have done for me throughout the years.

To Bryan, who drove me crazy but kept me from going insane.

And finally to Scott, a mumbling genius with a mischievous grin, an enormous heart, and plenty of bad ideas, who taught me lessons you can't learn in classrooms or textbooks.

For the ones who have loved me, supported me, made me laugh, made me cry, and have been by my side.

TABLE OF CONTENTS

Chapter Page

I. INTRODUCTION 1

1.1. Einstein, Schrödinger, and Entanglement 1

1.2. Entanglement in Quantum Information 4

1.2.1. The Difficulty of Verifying Entanglement 5

1.3. Overview 5

II. ENTANGLEMENT BASICS 8

2.1. Defining Entanglement 8

2.2. What Is It That's Entangled? 9

2.3. Entanglement Criteria 10

2.4. The Need for Many Copies 11

2.5. Local Operations and Classical Communication 11

III. VERIFYING ENTANGLEMENT IN THE HONG-OU-MANDEL DIP 13

3.1. Introduction 13

3.2. Entanglement Verification for Single-Mode States 15

3.2.1. Defining "Single Mode" 15

3.2.2. Local Filtering 16

Chapter Page

3.2.3. Entanglement Criterion 18
3.2.4. An Additional Phase Shift 19
3.2.5. Asymmetric Beamsplitters 22
3.2.6. Losses 22
3.3. Considerations Concerning Multi-Mode Multi-Photon States . 22
3.3.1. A Corrected Entanglement Criterion 23
3.3.2. Nonexistence of Local Filters for Sameness of Modes 24
3.3.3. An Alternative Local Operation 25
3.4. Summary 27

IV. MISSING DATA OUTSIDE THE DETECTOR RANGE: ITS IMPORTANCE FOR CONTINUOUS VARIABLE ENTANGLEMENT VERIFICATION AND QUANTUM CRYPTOGRAPHY 29

4.1. Introduction 29
4.2. Detecting Continuous-Variable Entanglement 30
4.2.1. Entanglement Criteria 30
4.2.2. Coarse Grained Measurements 31
4.2.3. Finite Range Detectors 33
4.3. Worst-Case Analysis 34
4.3.1. Assumptions 34
4.3.2. Smoothed EPR State 36
4.3.3. Renyi Entropies 37
4.3.4. Numerical Examples 39
4.3.5. The Cutoff Assumption 41
4.3.6. Smooth Entropies 42

Chapter Page

4.4. Conclusions 43

V. MISSING DATA OUTSIDE THE DETECTOR RANGE: APPLICATION TO TIME-FREQUENCY ENTANGLEMENT . . 44

5.1. Introduction 44

5.2. Measurements 46

5.2.1. Frequency Measurements 46

5.2.2. Time Measurements (Using Time to Frequency Conversion) . 47

5.2.3. Cutoff and Missing Data 49

5.3. Verifying Entanglement 49

5.4. Ideal State 51

5.5. Noise 54

5.6. Conclusions 58

VI. CONCLUSIONS 60

REFERENCES CITED 62

LIST OF FIGURES

Figure Page

1.1. The set of all states contains separable (yellow) and entangled (green) states. The darker the shade of green the more assumptions are allowed in verifying that class of states (e.g., verifying entanglement assumes the validity of quantum mechanics and that the measurements of Alice and Bob are known, whereas to verify Bell-nonlocality one cannot assume the validity of quantum mechanics, nor does one assume to know what Alice and Bob measure). Each green set also contains all lighter colored green sets. Not all properties are represented in this simplified depiction, but it does convey the convexity of the sets. Namely, the set of all states and the set of separable states are convex, while the set of entangled states is not. 3

3.1. Scatter plot of the right-hand side vs the left-hand side of our entanglement criterion (3.8). Red dots lie on the boundary of entangled vs separable, and correspond to pure separable states of the form $(|0\rangle_A + a|2\rangle_A) \otimes (|0\rangle_B + b|2\rangle_B)$ where a and b are real. Blue triangles corresponds to mixtures of two randomly generated separable states of the form $(|0\rangle_A + a_1|1\rangle_A + a_2|2\rangle_A) \otimes (|0\rangle_B + b_1|1\rangle_B + b_2|2\rangle_B)$ (with complex coefficients). 20

3.2. $\left[Q_{1,1} - \frac{1}{2}(P_{2,0} + P_{0,2})\right]^2$, that is, the right-hand side of inequality (3.8), for the state ρ_1 (top), defined in (3.9), and the more noisy ρ_2 (bottom), defined in (3.10), as a function of a phase shift $\exp(i\phi)$ applied to the first mode. The shaded region represents for which values of ϕ entanglement will be detected by ineq. (3.8) [both states are entangled for any value of ϕ]. 21

4.1. U_-^Δ for mixed separable state, where the missed counts outside the detector range have been ignored (the graph for V_+^δ would look identical). We would falsely conclude we have entanglement. Note the barely visible background level of counts: in order to properly reach conclusions about entanglement, we would need to know how far those background counts extend outside our detector range. . . 35

4.2. Left: Cartoon showing how to deal with missing data (red) outside our detector range for a *variance*-based entanglement or security criterion. After having determined a cutoff range beyond which we expect no counts, missed data are assigned to the outside bins within the cutoff range. Right: Same for an *entropic* entanglement or security criterion: missed data are as uniformly distributed as possible within the cutoff range. 36

4.3. Left: $|\Psi(u_a, u_b)|^2$ for the smoothed EPR state (4.7) with $\bar{n} = 1$; Right: $|\Psi(v_a, v_b)|^2$ for the same smoothed EPR state as measured by detectors with a 32 bin resolution. 37

4.4. Optimized Renyi criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the number of bins inside the detection range. One needs a minimum number of 7 bins to verify entanglement. 39

4.5. Optimized criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the detection cutoff C, which assumes no detection events would occur outside the interval $[-C, C]$). One needs $C < 21.5$ in order to be able to verify entanglement. 40

4.6. Optimized criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the detector range $[-R, R]$ with a fixed outer cutoff of [-10,10]. Entanglement can only be verified when the detection range is larger than [-1.9,1.9]. 41

5.1. Left: Continuous joint spectral probability, $|f(\omega_A, \omega_B)|^2$ Right: Binned joint temporal probability, $|\tilde{f}(t_A, t_B)|^2$, as measured with detectors with D=16 bins. 52

5.2. Probability of detection for each bin of Bob's detector, conditioned on Alice also detecting a photon. $\beta_+ = 3/4$ was chosen such that this is "reasonably flat". 53

5.3. Optimized entanglement criteria, M, as a function of the outer cutoff, where the outer cutoff in units of $\Delta/2$ ($\Delta = \Delta\omega, \Delta t$). Entanglement is verified for outer cutoffs less than $[-4.8(\frac{\Delta}{2}), 4.8(\frac{\Delta}{2})]$. 54

5.4. Left: Measured joint probability distribution for the state with time of arrival noise with $\sigma_\tau = 1.5\sigma_-$ Right: $T_-^{\delta t}$. Blue represents the original state with no noise, described by Eq. 5.16. Red is the state with time of arrival noise with $\sigma_\tau = 1.5\sigma_-$. While it may not appear that noisy, the red state will fail to be verified by the criteria. 56

Figure Page

5.5. Optimized entanglement criteria M as a function of σ_τ/σ_- for states with time of arrival noise. Entanglement is verified when $\sigma_\tau/\sigma_- \lesssim 1.17$. . 57

5.6. Optimized criterion M for states with both time and frequency noise. Entanglement is verified for colored area ($M < 0$). 58

CHAPTER I

INTRODUCTION

1.1. Einstein, Schrödinger, and entanglement

Entanglement was recognized as a counterintuitive property of quantum mechanics, and as such disliked by, for example, Einstein and Schrödinger. It became the subject of much disagreement and discussion. Einstein, Podolsky, and Rosen (EPR) famously wondered if a quantum-mechanical description of physical reality could be complete [1], and concluded that it could not. In their 1935 paper they described, as an example highlighting their objections, a two-particle system with a (non-normalizable, 1D) wavefunction

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} \mathrm{d}p \, \exp[(2\pi i/h)(x_1 - x_2 + x_0)p]. \tag{1.1}$$

The authors found it objectionable that for this state one could measure either the position or momentum of one particle and then predict, *with certainty*, the value of the same quantity of the other particle, despite the fact that the particles were separated and no longer interacting. This seemed to imply that the other particle already must have had a particular position *and* a particular momentum, even though the quantum-mechanical wavefunction certainly cannot ascribe both values precisely (position and momentum being described by non-commuting observables, according to quantum mechanics). Hence, quantum mechanics (i.e., a description based on just the wavefunction) must be incomplete, so concluded EPR.

Today we recognize the state Ψ as being entangled—and we call it the EPR state!—but the term "entanglement" (or rather, its German counterpart,

"Verschränkung") was not coined until later that year by Schrödinger in response to such discussions [2]. Schrödinger was also not satisfied with the implications of entanglement:

> Attention has recently been called to the obvious but very disconcerting fact that even though we restrict the disentangling measurements to one system, the representative obtained for the other system is by no means independent of the particular choice of observations which we select for that purpose and which by the way are entirely arbitrary. It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it.

We now know that quantum mechanics cannot be an incomplete version of any local, realistic theory (where by "realistic" we mean that physical systems possess properties independent of whether they are measured or not [3]). In 1964 John Bell showed explicitly that local realism and quantum mechanics are incompatible theories, and that, in some situations, a local hidden variable model and quantum mechanics will offer different predictions of experimental outcomes [4]. This led to experimentally testable inequalities ("Bell inequalities") which any state described by a local hidden variable model must satisfy, but which can be violated by certain states described by quantum mechanics. Such states that violate the Bell inequalities must be entangled. A loophole free demonstration of such a violation has not yet been achieved, but so far the evidence is overwhelmingly in favor of quantum mechanics. A modern use of Bell inequalities is as a way of verifying that a state is entangled, although "Bell-nonlocality" is a stronger condition than being entangled in the sense that not all entangled states will violate Bell-type inequalities.

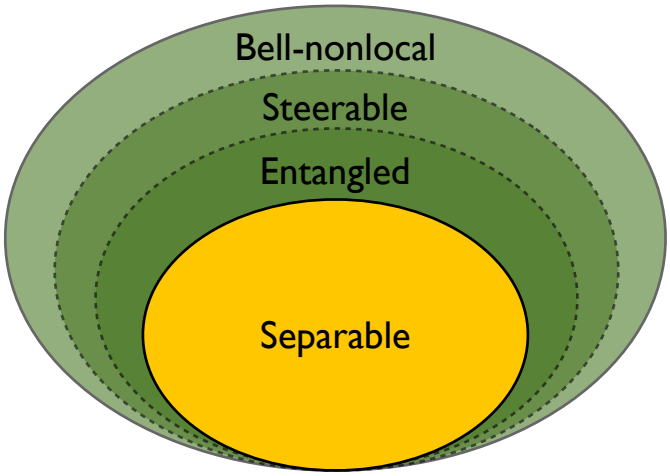

FIGURE 1.1. The set of all states contains separable (yellow) and entangled (green) states. The darker the shade of green the more assumptions are allowed in verifying that class of states (e.g., verifying entanglement assumes the validity of quantum mechanics and that the measurements of Alice and Bob are known, whereas to verify Bell-nonlocality one cannot assume the validity of quantum mechanics, nor does one assume to know what Alice and Bob measure). Each green set also contains all lighter colored green sets. Not all properties are represented in this simplified depiction, but it does convey the convexity of the sets. Namely, the set of all states and the set of separable states are convex, while the set of entangled states is not.

The concept of steering first introduced by Schrödinger (see the above quote) has since been formalized and experimentally demonstrated [5, 6]. This has also led to "steering inequalities" [7], a violation of which indicates a state is steerable. Like the Bell inequalities, they are only violated by entangled states and, therefore, can be used to verify entanglement. The steering inequalities are weaker than the Bell inequalities, i.e., there are states that will violate the steering inequalities but not the Bell inequalities, but stronger than entanglement conditions. The set of all entangled states contains the set of all steerable states which contains the set of all Bell-nonlocal states. This is depicted in Figure 1.1.

1.2. Entanglement in quantum information

With the advent of quantum information processing, entanglement was elevated from a novel phenomenon and subject of debate to a *valuable resource*. Entanglement is either provably helpful or believed to be necessary for many of the tasks of quantum information such as quantum computing, teleportation, quantum key distribution, and others. Quantum computing offers the ability to solve certain problems quickly[1] which are not believed to be efficiently solvable by classical computation [8]. One important example of this is Shor's algorithm [9] which allows large numbers to be factored quickly by a quantum computer, something which is not believed to be possible with a classical computer [8]. This current inability to efficiently factor large numbers is the source of security for most most modern cryptographic schemes, such as RSA [10]. If a quantum computer were to be developed, these protocols would no longer be secure and new cryptographic methods would have to be used. This is a motivation for the development of quantum key distribution (QKD), which is provably secure regardless of any advances in quantum computing.

With the increasing importance of entangled states came a need for ways to verify, quantify, and characterize entanglement. Our interest is in the easiest of these tasks, the verification of entanglement, specifically verification of bipartite entanglement. Even this is still non-trivial as given a density matrix it is NP-hard to verify that it is entangled [11]. We will focus on bipartite optical entanglement in this dissertation. For many years polarization entangled photon pairs were a popular resource for demonstrating Bell inequality violations [12], teleportation [13], QKD [14], steering [6], etc. These states are easy to generate and well understood, but they aren't ideally

[1]By 'quickly' and 'efficiently' we mean the time required to solve the problem is polynomial in the size of the input (measured in bits).

suited for all tasks. More recently there has been increasing interest in generating and utilizing other forms of optical entanglement [15–17], for example to encode more than one bit per photon.

1.2.1. The difficulty of verifying entanglement

The theoretical problem of deciding if a state specified by a given density matrix is entangled is a hard problem, and experimental entanglement verification is made even harder by the practical issues that arise in performing an experiment in a lab. Applying the theoretical methods of entanglement verification to experiments is often not as straightforward as one would initially think or hope. Indeed, some theoretical methods of verifying entanglement have been inappropriately applied to experimental results, leading to false claims of having verified entanglement (that is, all data could be explained by unentangled states), as in, for example, Ref. [18]. Some methods are simply too difficult to be feasible or practical (e.g. those that require full state tomography for large dimensional systems), while others may on the surface seem easy to apply, but rely on assumptions that are not warranted [19]. Ignoring these issues is at best unwise, and at worst potentially dangerous. The danger is most obvious in the cryptographic setting where the two parties (conventionally called Alice and Bob) should abort their protocol if they cannot prove entanglement (and thereby security). If they falsely believe they have security, they will not abort, leaving them vulnerable to eavesdropping attacks.

1.3. Overview

This dissertation will explore the problem of entanglement verification for two different kinds of photonic states relevant to quantum information processing for

which conventional methods do not work well. One type of state occurs in Hong-Ou-Mandel interference, the other concerns time-frequency entanglement. We will develop new methods and criteria for these states, and we will attempt to do so in a way that is straightforward and easy to experimentally implement.

This dissertation is structured as follows:

In Chapter II we briefly discuss the basics of entanglement needed for the following chapters.

In Chapter III we look at verifying the entanglement of states similar to the delocalized photon pair that occurs due to Hong-Ou-Mandel interference [20]. This interference occurs when two photons (usually assumed to be identical in every way except propagation direction, but for an interesting exception see [21]) are incident on the two inputs of a 50/50 beam splitter and always exit together (thus revealing the bosonic character of photons). This type of interference is important for quantum computing schemes based on linear optics [22–24].

Chapter IV discusses continuous variable entanglement of photon pairs. We look at the general problem of how to verify entanglement using measurements made with detectors with finite range and how the data missed by these detectors affects our ability to verify entanglement. As an example we look at a smoothed, normalized version of the EPR state that we encountered in Eq. (1.1).

In Chapter V we apply the techniques developed in the previous chapter to a recently proposed quantum key distribution scheme [25] based on time-frequency entangled photon pairs as in that scheme missing data plays an important role. We also examine how generic forms of noise affect our ability to verify entanglement in this case.

Chapter VI summarizes the results of this dissertation, puts the results into context, and briefly indicates what is new.

Chapter III was published and co-authored with S. J. van Enk. Chapter IV and Chapter V have been submitted for publication and co-authored with S. J. van Enk.

CHAPTER II

ENTANGLEMENT BASICS

Here we will provide some of the necessary background for the remaining chapters by discussing several basic features of entanglement. We will restrict ourselves to the case of bipartite entanglement.

2.1. Defining entanglement

The pure state of a bipartite system with spatially separated subsystems A and B (held by Alice and Bob, respectively), denoted by $|\Psi\rangle_{AB}$, is said to be separable if it can be written as a product of states describing the subsystems A and B

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi'\rangle_B \,. \tag{2.1}$$

If it cannot be written in such a form it is called entangled. A textbook example of a pure, bipartite entangled state is the spin singlet state

$$|\Psi\rangle = (|\uparrow\rangle_A |\downarrow\rangle_B - |\downarrow\rangle_A |\uparrow\rangle_B)/\sqrt{2}. \tag{2.2}$$

The definitions of separable and entangled can be extended to mixed states as follows. A mixed state, represented by a density matrix ρ_{AB}, is said to be separable if it can be written as a probabilistic mixture of separable pure states

$$\rho_{AB} = \sum_i p_i \, \rho_A^i \otimes \rho_B^i, \tag{2.3}$$

where

$$\rho_j^i = |\psi^i\rangle_j \langle\psi^i| \tag{2.4}$$

for $j = A, B$, with $\sum_i p_i = 1$ and $p_i \geq 0$. The p_i's can be interpreted as probabilities. Such states may describe classically correlated systems. If a state can not be written in such a form, it is called entangled.

2.2. What is it that's entangled?

We will consider entangled states of electromagnetic fields. While it may be tempting to think of such entanglement as being between photons (or more broadly as between particles), that is not generally the case. The entanglement is actually between modes[1] [26]. Consider, for example, the state

$$|\Psi\rangle = (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)/\sqrt{2}, \tag{2.5}$$

where $|n\rangle_j$ are the number states of the spatially separated modes $j = A, B$. This state only has a single (delocalized) photon, but the state is indeed entangled. Specifically, modes A and B are entangled.

If the two separate locations each have a fixed number of photons then we can, for convenience, refer to the entanglement as being between the photons. One example of such an entangled state is the two-photon polarization entangled state

$$|\Psi\rangle = (|\updownarrow\rangle_A |\leftrightarrow\rangle_B - |\leftrightarrow\rangle_A |\updownarrow\rangle_B)/\sqrt{2}, \tag{2.6}$$

[1] 'Mode', briefly, is defined as follows: Expand $\vec{E}$ in some complete set of solutions. Each one solution from this set corresponds to a mode.

or, in Fock state notation,

$$|\Psi\rangle = (|1\rangle_{A,H}|0\rangle_{A,V}|0\rangle_{B,H}|1\rangle_{B,V} - |0\rangle_{A,H}|1\rangle_{A,V}|1\rangle_{B,H}|0\rangle_{B,V})/\sqrt{2}. \tag{2.7}$$

In this case Alice's and Bob's modes each have exactly one photon in total, so it is reasonable (but not necessary) to talk about the entanglement being between "photon A" and "photon B."

2.3. Entanglement criteria

Given a bipartite density matrix ρ_{AB}, how does one decide if it is separable or entangled? This is, in general, a hard problem (NP hard, in fact [11]). For 2x2 and 2x3 dimensional systems, the positive partial transpose (PPT) criterion [27, 28] is both necessary and sufficient for ρ_{AB} to be separable, but for higher dimensional systems there is no known test that can conclusively identify any given state as being either separable or entangled.

Given the choice between overestimating or underestimating entanglement, the latter is strongly preferred. This is especially clear in the context of quantum cryptography. While entanglement is not required for implementing quantum key distribution, secure quantum key distribution requires the ability of the sender and receiver to use their measurement results to prove the presence of entanglement in the effective quantum state distributed between them [29]. Likewise, we are not interested in trying to prove that we do not have entanglement, but rather prove that we do.

With this in mind, entanglement criteria classify a state as being either a) entangled or b) possibly separable, possibly entangled. While for any given entanglement criterion some entangled states will not be identified as such (assuming

the state is not of the low dimensions described above), when experimentally trying to verify a state as entangled, the experimentalist typically knows what kind of entangled state they hope to generate (since they presumably designed their experiment to produce a specific kind of state). So they can improve their chances of successfully verifying the entanglement of the state they have prepared (if it is actually entangled) by choosing a criterion that would verify entanglement for the targeted ideal state.

2.4. The need for many copies

No measurement on a single copy of a state can verify entanglement. Entanglement is not an observable. For example, for a pure state, entanglement is quantified as

$$E_{AB} = -Tr\rho_A \ln \rho_A, \tag{2.8}$$

where $\rho_A = Tr_B\rho_{AB}$ is the reduced density matrix for system A, which shows entanglement is a *nonlinear* function of the state. One must have many copies and make many measurements before anything definite can be said. A finite number of measurements cannot say with 100 % certainty that a state is entangled, but rather that it is with some probability. This is discussed in more detail in Ref. [30].

2.5. Local operations and classical communication

Entanglement is quantified in such a way that the amount of entanglement of a state cannot, on average, increase due to local operations and/or classical communication. We say "on average" because *some* measurement outcomes may increase the amount of entanglement (and other outcomes then necessarily decrease it). This fact about quantifying entanglement is relevant to the process of verifying entanglement in that this allows Alice and Bob to perform local operations on their

respective systems, A and B, and to communicate as much classical information as they please without risking concluding incorrectly their shared state is entangled.

CHAPTER III

VERIFYING ENTANGLEMENT IN THE HONG-OU-MANDEL DIP

This work was published as *Verifying entanglement in the Hong-Ou-Mandel dip*, Physical Review A **83**, 042318 (2011). It was initiated by S. J. van Enk and finished jointly by Megan R. Ray and S. J. van Enk.

3.1. Introduction

Quantum interference effects that arise when single photons impinge on a beam splitter are crucial to linear-optics quantum computing schemes [22–24], with the other indispensable *non*linear ingredient provided by photon-counting measurements. One such linear-optics quantum interference effect was observed for the first time in 1987, by Hong, Ou, and Mandel, and it still carries their name [20]. In the Hong-Ou-Mandel interference (HOMi) effect, two photons in otherwise identical modes impinge on two different input ports of a 50/50 beam splitter, and, thanks to bosonic interference, always emerge together in one of the two output ports. More precisely, the output state can be expressed in Fock states as

$$|\Psi\rangle_{AB} = (|0\rangle_A |2\rangle_B - |2\rangle_A |0\rangle_B)/\sqrt{2}. \tag{3.1}$$

Here A and B denote the two output modes, with identical polarizations, frequencies, and transverse spatial quantum numbers, and differing only in their propagation directions. Great progress has been made recently in building waveguide circuits on chips, with which high-visibility interference fringes involving multi-photon states with high purity such as $|\Psi\rangle$ can be observed [31].

The aspect of the output state $|\Psi\rangle_{AB}$ that interests us here is that it, provided the modes A and B are spatially separated, is entangled. For instance, the pure state $|\Psi\rangle$ can be shown to violate Bell-type inequalities [32]. What concerns us in particular, is how one could verify the entanglement of noisy versions of the ideal state, containing, e.g., phase noise and contaminations with states with different numbers of photons (no photons at all, one photon in total, or more than two photons in total). As it turns out, standard measurements and operations used in, e.g., [31] to characterize and manipulate few-photon states are indeed sufficient for entanglement verification, provided (but this is a far from trivial proviso) all photo detectors detect photons only in particular modes. That is, if we assume our detectors are sensitive only to one particular polarization, spectral amplitude, and transverse spatial mode, then the method we present here will unambiguously detect entanglement even if the actual input state (with arbitrary numbers of photons in it) has a multi-mode character. Moreover, in this case we can construct lower bounds on the amount of entanglement as well. The reason is that such a detection scheme is equivalent to a protocol where a filtering operation is applied to the input state that keeps only photons in the desired modes. Since this operation is *local*, the amount of entanglement of the resulting filtered state cannot be larger, on average, than the entanglement present in the input state.

On the other hand, if we drop the assumption about the single-mode character of our detection devices, then the problem of verifying entanglement of a delocalized two-photon state becomes much more involved, also when compared to the similar problem of verifying entanglement of a delocalized *single* photon [33, 34]. We will give the essential reason for this difference and present solutions for the multi-mode

multi-photon entanglement verification problem that will work if the state under investigation is sufficiently close to a single-mode entangled state.

It may be interesting to compare our entanglement verification scheme to a scheme proposed in Refs. [35, 36], which likewise uses the HOM interference effect (but in its fermionic version) to detect entanglement. The latter scheme detects entanglement between electrons, and assumes the number of electrons in each input port of a 50/50 beamsplitter is fixed and known, whereas we do not assume a fixed photon number. Indeed, such an assumption is perfectly fine for first-quantized electrons, but not for second-quantized photons. Moreover, we use the *inverse* HOM effect to detect entanglement in a state: ideally, we have either two photons or no photons in each input mode, whereas Refs. [35, 36] consider, in the ideal case, one electron in each input mode, and then use the proper HOM effect for entanglement detection.

Finally, we recall that the (proper) HOM effect has been used to detect entanglement between two input photons (see, e.g., Ref. [37] and references therein). It's still true that the assumption that there is exactly one photon in each input port is not warranted in general, but, for entanglement verification, it is an allowed filtering operation, as it is local. In contrast, filtering on having two photons in total in the two input ports (which operation we would like to perform for our case) would be nonlocal.

3.2. Entanglement verification for single-mode states

3.2.1. Defining "single mode"

Let us first consider so-called single mode states, by which we mean states where any photons present are in the same transverse spatial, spectral, and polarization

modes, with the understanding that they can differ in their direction of propagation (there are two such modes in our case, spatially separated, which we call modes A and B). Since experiments typically must be repeated in time, we do allow the spectral mode functions $\phi(\omega)$ to differ by a phase factor $\exp(i\omega T)$ with T a *known* delay time, without the photons losing their single-mode character.

We could, in principle, perform tomography on the full state to determine its density matrix and from this calculate a measure of entanglement, e.g., the concurrence or negativity of the state, and thus determine whether the state is entangled. However, since we shouldn't assume anything about the Hilbert space that the state lives in (since we want be able to verify the entanglement on noisy versions of our ideal state), we would have an infinite number of matrix elements to determine. Even if we were to make restrictive assumptions about the Hilbert space of the state, it would still require numerous measurements to fully determine the state. For example, if we assumed that the state did not contain more than two photons, this would still leave a 6x6 density matrix to determine. If we are not interested in fully characterizing the state, but merely in verifying its entanglement we do not need to do so much work. Instead of trying to exactly calculate a measure of entanglement of the state, we can instead calculate a lower bound which will allow verification of entanglement of the state with far fewer measurements.

3.2.2. Local filtering

Let the state whose entanglement we are trying to verify be called ρ. A bound on the entanglement can be found in the following way. Suppose we were to apply the following *local* filtering operations: we ask about each of the two spatially separated

modes A and B two questions

Filter "**1**" : Is there exactly 1 photon in the mode?

Filter "**2**" : Are there more than 2 photons in the mode?

We consider this filtering a success if the answer is "no" to both questions [cf. Eq. (3.1)]. The probability then of successful filtering is $\tilde{P} = P_{0,0} + P_{0,2} + P_{2,0} + P_{2,2}$, where $P_{i,j}$ is the probability to find i photons in mode A and j photons in mode B in the unfiltered state ρ. This filtering collapses our state to one living in the smaller Hilbert space spanned by $|0\rangle_A|0\rangle_B$, $|0\rangle_A|2\rangle_B$, $|2\rangle_A|0\rangle_B$, and $|2\rangle_A|2\rangle_B$. At this point we have a state represented by a density matrix with up to 16 nonzero elements. To simplify calculations we can further bound the state's entanglement by assuming we apply another local operation, which in addition requires classical communication:

Local operation + classical communication : "**phaseshift**" :

apply the same random phase shift to both modes

thus destroying any coherence between states with different numbers of photons and reducing the number of nonzero matrix elements to at most 6.

3.2.3. Entanglement criterion

The end result of filtering is of the (normalized) form

$$\tilde{\rho} = \frac{1}{\tilde{P}} \begin{pmatrix} P_0 & 0 & 0 & 0 \\ 0 & P_{0,2} & d & 0 \\ 0 & d^* & P_{2,0} & 0 \\ 0 & 0 & 0 & P_{2,2} \end{pmatrix} \tag{3.2}$$

Since concurrence is an entanglement monotone and $\tilde{\rho}$ is the result of only local operations and classical communication applied to ρ, the concurrence of $\tilde{\rho}$ bounds the concurrence of ρ: $\tilde{P}C(\tilde{\rho}) \leq C(\rho)$. The concurrence of $\tilde{\rho}$ is

$$\tilde{P}C(\tilde{\rho}) = \max[\,0,\; 2|d| - 2\sqrt{P_0 P_{2,2}}\,] \tag{3.3}$$

which is greater than zero when

$$P_0 P_{2,2} < |d|^2. \tag{3.4}$$

Thus $\tilde{\rho}$ is provably entangled if ineq. (3.4) holds true, and so too is ρ. Similarly, since negativity is also an entanglement monotone, the negativity of $\tilde{\rho}$ bounds the negativity of ρ in the same way: $\tilde{P}\mathcal{N}(\tilde{\rho}) \leq \mathcal{N}(\rho)$. But calculating the negativity of $\tilde{\rho}$ results in exactly the same bound as found by calculating the concurrence: the state is provably entangled if $P_0 P_{2,2} < |d|^2$.

Now we must find a way to bound $|d|^2$. Since $d = \tilde{P}\langle 02|\tilde{\rho}|20\rangle = \langle 02|\rho|20\rangle$ we don't need to physically perform any of the filtering mentioned above, as we can determine the needed information, d, from the unfiltered state ρ. To do this, consider placing

the two modes of ρ on the two input ports of a lossless 50/50 beamsplitter. We will label the input modes A and B, and the output modes C and D. The transformation between input mode creation operators and output creation operators can be written as follows (after adding, for convenience, a $\pi/2$ phase shift to mode D to compensate for the $\pi/2$ phase shift upon reflection)

$$a^\dagger \to \frac{c^\dagger + d^\dagger}{\sqrt{2}} \qquad \text{and} \qquad b^\dagger \to \frac{c^\dagger - d^\dagger}{\sqrt{2}} \tag{3.5}$$

which allows us to calculate photo-detection probabilities $Q_{i,j}$ for the output modes, where $Q_{i,j}$ is the probability to find i photons in mode C and j photons in mode D. It can be shown that

$$Q_{1,1} = \frac{1}{2}\left(P_{2,0} + P_{0,2} - d - d^*\right), \tag{3.6}$$

which gives

$$\left(Q_{1,1} - \frac{P_{2,0} + P_{0,2}}{2}\right)^2 = \left(\frac{d + d^*}{2}\right)^2 = \Re(d)^2 \leq |d|^2. \tag{3.7}$$

So when

$$P_0 P_{2,2} < \left(Q_{1,1} - \frac{P_{2,0} + P_{0,2}}{2}\right)^2 \tag{3.8}$$

the state can be said to be provably entangled. Figure 3.1. plots both sides of our inequality (3.8) for many randomly picked separable states, to show how this criterion indeed verifies entanglement. Moreover, the figure caption identifies the states lying on the borderline between separable and verifiably entangled.

3.2.4. An additional phase shift

Our condition (3.8) will not detect entanglement in an input state, even when it is in fact present, when d is largely or purely imaginary. But if one were to apply

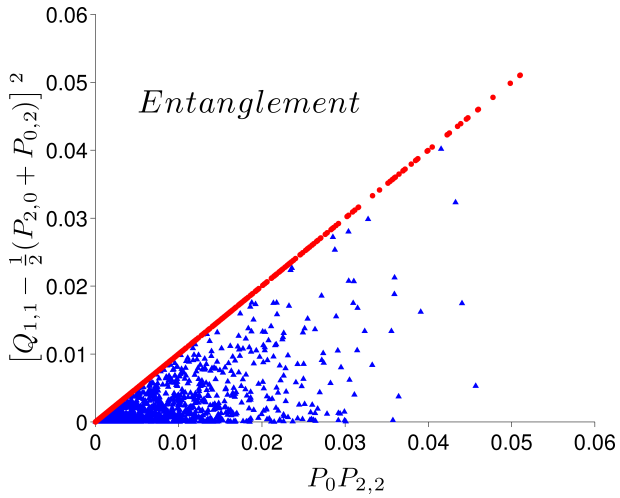

FIGURE 3.1. Scatter plot of the right-hand side vs the left-hand side of our entanglement criterion (3.8). Red dots lie on the boundary of entangled vs separable, and correspond to pure separable states of the form $(|0\rangle_A + a|2\rangle_A) \otimes (|0\rangle_B + b|2\rangle_B)$ where a and b are real. Blue triangles corresponds to mixtures of two randomly generated separable states of the form $(|0\rangle_A + a_1|1\rangle_A + a_2|2\rangle_A) \otimes (|0\rangle_B + b_1|1\rangle_B + b_2|2\rangle_B)$ (with complex coefficients).

a phase shift to one of the modes before placing the state on the beam splitter and vary that phase until $Q_{1,1}$ was maximized (the same local operation with classical communication as performed in [31]), this would maximize $\Re(d)^2$, thus making ineq. (3.4) equivalent to (3.8). In other words, such states then can be detected by our criterion. Take, for instance, the state

$$\rho_1 := \frac{1}{6} |00\rangle \langle 00| + \frac{1}{3}(|20\rangle + i\,|02\rangle)(\langle 20| - i\,\langle 02|) + \frac{1}{6} |22\rangle \langle 22| \,. \tag{3.9}$$

For this state $|d|^2 = \frac{1}{9}$ and $P_0P_{2,2} = \frac{1}{36}$ so by ineq. (3.4) the state is in fact entangled. However $\Re(d)^2 = 0$, so ineq. (3.8) will not detect the entanglement. But if we apply a phase shift of $\exp(i\frac{\pi}{2})$ to one of the modes then d will become purely real (and so $Q_{1,1}$ will be maximized), and ineq. (3.8) *will* detect the entanglement. As Figure 3.2. (top) shows, for this state with a phase $\exp(i\phi)$ applied to the first mode, entanglement

will be detected when ϕ is between $\frac{1}{6}\pi$ and $\frac{5}{6}\pi$ or between $\frac{7}{6}\pi$ and $\frac{11}{6}\pi$. A similar, but more noisy state,

$$\rho_2 := \frac{1}{3}\left|00\right\rangle\left\langle 00\right| + \frac{1}{4}(\left|20\right\rangle + i\left|02\right\rangle)(\left\langle 20\right| - i\left\langle 02\right|) + \frac{1}{6}\left|22\right\rangle\left\langle 22\right|, \tag{3.10}$$

will have a smaller range of detectable entanglement, specifically when ϕ is between $.39\pi$ and $.61\pi$ or between 1.39π and 1.61π (see Figure 3.2., bottom part).

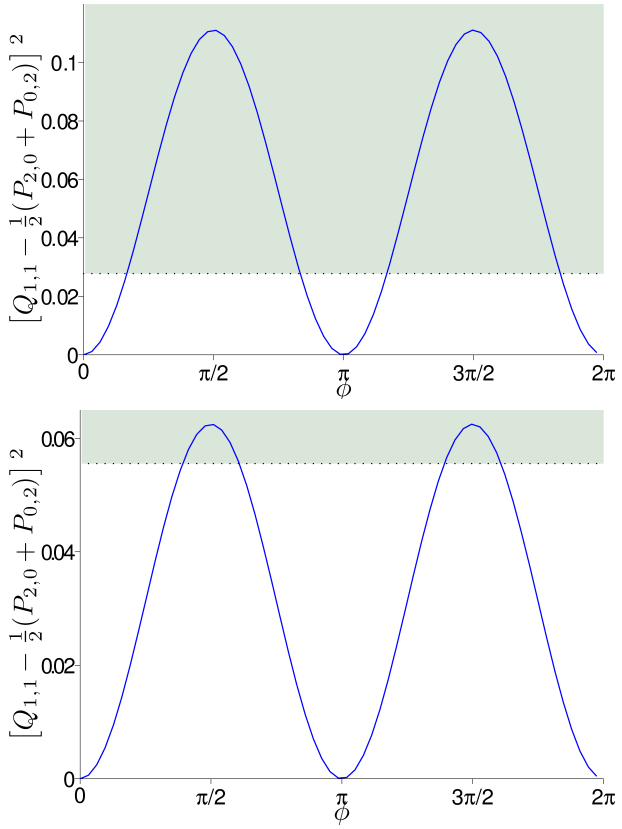

FIGURE 3.2. $\left[Q_{1,1} - \frac{1}{2}(P_{2,0} + P_{0,2})\right]^2$, that is, the right-hand side of inequality (3.8), for the state ρ_1 (top), defined in (3.9), and the more noisy ρ_2 (bottom), defined in (3.10), as a function of a phase shift $\exp(i\phi)$ applied to the first mode. The shaded region represents for which values of ϕ entanglement will be detected by ineq. (3.8) [both states are entangled for any value of ϕ].

3.2.5. Asymmetric beamsplitters

To bound d we placed our state on a 50/50 beamsplitter, but it is easy to generalize our analysis to beam spitters which are not equally balanced. Suppose our beam splitter has a (real) reflection coefficient r and a (real) transmission coefficient $t = \sqrt{1-r^2}$ such that the input creation operators transform as

$$a^\dagger \to rc^\dagger + td^\dagger \qquad \text{and} \qquad b^\dagger \to tc^\dagger - rd^\dagger \tag{3.11}$$

Following the same analysis as before we find that if

$$P_0 P_{2,2} < \left(\frac{Q_{1,1} + P_{1,1}(t^2 - r^2)}{4r^2 t^2} - \frac{P_{2,0} + P_{0,2}}{2} \right)^2 \tag{3.12}$$

the state is provably entangled.

3.2.6. Losses

We conclude this Section by noting that it is straightforward to take into account the influence of losses and inefficient photo detectors. Namely, *all* our measurements boil down to counting photons in the end (with the results being typically 0 or 1, sometimes 2, and rarely 3). Provided all loss rates and detector inefficiencies are known, one can infer the actual photon number distributions [to be used in inequalities (3.8) or (3.12)] from the measured distributions by inversion.

3.3. Considerations concerning multi-mode multi-photon states

We made the assumption at the beginning of our analysis that any photons present are in the same transverse spatial, spectral, and polarization mode. However

if our detectors only detect a certain single mode we can drop the assumption of the photons being in the same mode as this is equivalent to a local filtering. That is, using single mode detectors is equivalent to an additional filtering performed on each of the spatially separated modes, filtering out all photons not in the single mode of interest before detection takes place. What if we drop the assumption of single-mode detectors?

Suppose we have an input state in which the photons present are *not* all in the same transverse spatial, spectral, and polarization mode. The entanglement verification scheme described above did assume that the two photons in the filtered state (after the local filtering operations "1" and "2") are in the same mode, because of the explicit assumption that there is interference (of the "inverse HOM" type) taking place on a beam splitter. But this assumption does affect how we interpret the results of the measurements: in particular, the quantity Q_{11} (which we would like to be large) could be dangerously contaminated with contributions from those input states that lead to larger values of Q_{11} for photons in different modes than for photons in the same modes. For example, if we start with an output state with one photon in each output port, but of different colors, then applying the inverse beam-splitter transformation yields an input state that has this undesired property. The question is to what extent we can avoid or correct for the presence of such input states.

3.3.1. A corrected entanglement criterion

One way of correcting for these unwanted states is to subtract the contribution from the worst possible kind of state, i.e., one that maximizes the right hand side of

Eq. (3.8) without HOM entanglement, such as the state mentioned above

$$(|10\rangle_{red} + |01\rangle_{red}) \otimes (|10\rangle_{blue} - |01\rangle_{blue})\,/2 \tag{3.13}$$

While this state has twice as much entanglement as the HOM state, it is not the type of entanglement we are interested in trying to detect here. A state such as this with a probability P_2^o of detecting two photons of different color will contribute at most $3P_{1,1}^o/2$ to the quantity being squared on the rhs of Eq. (3.8), so we will compensate for this possible contribution by subtracting $3P_{1,1}^o/2$. For states close to the ideal state the contamination of different colored photons will be small and thus the correction will be small. We can also construct a bound that does not rely on measuring the probability of detecting two photons of different colors, since it is always less than or equal to the probability of detecting two photons of any color($P_{1,1}^o \leq P_{1,1}$.) Using this, our (conservative) condition for entanglement becomes

$$P_0 P_{2,2} < (\max[\, Q_{1,1} - P_{1,1} - P_2/2\,, 0\,])^2 \tag{3.14}$$

3.3.2. Nonexistence of local filters for sameness of modes

It would be nice if we could find a local filtering operation that checks whether two input photons propagating in one direction are in the same mode with respect to the other quantum numbers or not. There is certainly no von Neumann measurement that achieves that goal, as the target states are not all orthogonal. But, surprisingly, we cannot even construct a positive-operator valued measure (POVM) that does the trick: the reason is that even if we start with a state that contains two photons in orthogonal modes, say described by creation operators $a_1^\dagger$ and $a_2^\dagger$, then we can view

the same state as a superposition of two states, each with the two photons in identical modes, as described by the creation operators $a_{\pm}^{\dagger} = (a_1^{\dagger} \pm a_2^{\dagger})/\sqrt{2}$. This results from the identity

$$a_1^{\dagger} a_2^{\dagger} = \frac{(a_+^{\dagger})^2 - (a_-^{\dagger})^2}{2}. \tag{3.15}$$

This is then the essential difference between single-photon states and multi-photon states, which makes entanglement verification much harder for two-photon states than for single-photon states! Moreover, this also illustrates a difference between bosons and fermions: in the case of two fermions there *is* an antisymmetric subspace, and, e.g., we can certainly perform a measurement that checks whether two spin-1/2 systems have different spins (singlet state!) or not.

3.3.3. An alternative local operation

All is not quite lost, as we can still apply other sorts of local operations that are useful for the analysis of entanglement of the input state. In particular, suppose that our input state is some coherent superposition of, e.g., the desired state $(|0\rangle_A |2\rangle_B - |2\rangle_A |0\rangle_B)/\sqrt{2}$ and an unwanted state $|1\rangle_{A_1} |1\rangle_{A_2} |0\rangle_B$ (with photons in different modes). There is a local operation that transforms this superposition into an incoherent mixture of these two states: to each pair of orthogonal modes A_k and B_k (picked from some fixed basis: that's the essential difference from the no-go statement from the preceding subsection) apply a random k-dependent phase shift, and then forget the precise phase shifts applied. This operation will only preserve the coherence of superpositions of photons in the same spectral, polarization and transverse modes in A and B. That is, by a local operation we can transform the input state into a state of the form

$$\rho = P_s \rho^s + (1 - P_s)\rho^{\perp}, \tag{3.16}$$

where the first term denotes states that do display (inverse) HOM interference, and the second term states that do not; P_s is the probability of observing HOM interference, given ρ. The point is that we have now separated the input state in two parts, the first part of which is the state for which our method demonstrates entanglement (see below for further elaborations of this point). The second term has no entanglement, since any superpositions in that term have been destroyed. Its presence could imply the state ρ is not entangled, even if ρ^s is, namely if $1 - P_s$ is too large. We will not solve the (hard) general problem of identifying for what values of P_s and for what states ρ^s, entanglement of the latter still implies entanglement of ρ.

Let us return to the statement that ρ^s is entangled, if our verification method succeeded. We still have to discuss the fact that our method assumed that both photons are in one particular mode, whereas for photons in ρ^s we only know they are in the same mode, but not in which one. This does have consequences for the amount of entanglement (see [38] for extensive discussions of this issue), but not for the bare fact that the state is entangled. We can demonstrate this by showing that the state ρ^s can be distilled (the following protocol is far from optimal, and one can easily improve its efficiency; here its point is only an existence proof): just take two copies of ρ^s; first determine a particular mode such that the projection of ρ^s onto that mode is entangled; then perform on each of the A and B modes a joint measurement that counts how many photons in that particular mode there are in total in the two copies. If the answer is "2" for both A and B, we have an entangled state in that one particular mode. In this highly inefficient protocol the average amount of entanglement decreases (unless only a single mode is occupied), but it stays nonzero. Hence ρ^s must be entangled.

For clarity, let us add that the point of the distillation protocol is not that it would be used in an actual entanglement verification experiment. Instead, it is just a theoretical construct used to show that ρ^s must be entangled, by showing it contains a nonzero amount of distillable entanglement. For that limited theoretical purpose, it is sufficient to consider any suitable ideal protocol, including one that uses *single-mode* photo detectors.

3.4. Summary

We demonstrated how the inverse HOMi effect can be used to verify the mode entanglement present in a state of the form $(|0\rangle|2\rangle - |2\rangle|0\rangle)/\sqrt{2}$, and noisy versions thereof. If the photons in the state are all "single-mode", that is, all have the same polarization, the same transverse mode profile and the same spectral amplitude, then our method easily bounds the amount of entanglement from below. That directly gives a criterion, inequality (3.8), which, when satisfied for a given single-mode state, is sufficient to prove entanglement. We analyzed how the applicability of the criterion can be improved simply by applying an additional phase shift to one of the two modes. The operations needed to verify entanglement can be implemented with linear optics, and are just those demonstrated in the experiment of [31].

We discussed how the problem of verifying entanglement in the delocalized two-photon state with the inverse HOMi effect becomes more "interesting" (a euphemism for "complicated") without this single-mode assumption [more precisely, when both the input state *and* one's photo detectors are multi-mode], and why a delocalized single-photon state does not suffer from these complications. On the other hand, the interpretation of violating a Bell inequality with unbalanced homodyne measurements [32] is immune to the single-mode or multi-mode character of the input state, at the

small cost of requiring phase-locked local oscillators, thus showing an advantage of Bell inequalities in the context of entanglement verification.

We gave a simple solution to the full problem of inverse HOMi multi-mode multi-photon mode entanglement, based on bounding the deviation of the actual state from a single-mode state. This solution works well when that deviation is sufficiently small. It yields an entanglement criterion (3.14), similar to, but more conservative than (3.8).

CHAPTER IV

MISSING DATA OUTSIDE THE DETECTOR RANGE: ITS IMPORTANCE FOR CONTINUOUS VARIABLE ENTANGLEMENT VERIFICATION AND QUANTUM CRYPTOGRAPHY

This work has been accepted for publication in Physical Review A. It was initiated by S. J. van Enk and finished jointly by Megan R. Ray and S. J. van Enk.

4.1. Introduction

Secure quantum key distribution requires the ability of the sender and receiver to use their measurement results to prove the presence of entanglement in the (effective[1]) quantum state distributed between them [29]. The problem of how to decide whether a given state is separable or entangled continues to be an area of active research [39]. In almost all applications it is important to avoid concluding there is entanglement when there is, in fact, none. In other words, false positives are considered considerably worse than false negatives.

There has been great interest in continuous-variable (CV) entanglement for quantum information processing (for example, for a handful of very recent experiments, see Refs. [40–44]). One reason is that within the research area of quantum optics, CV states such as coherent states or two-mode squeezed states are easier to generate than single-photon polarization states. Moreover, by using

[1]In the case of prepare and measure schemes using single photons with no entanglement, the signal preparation process is equivalent (for the purpose of security analysis) to Alice preparing an entangled two photon state of the form $|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}\,|\alpha_i\rangle\,|\phi_i\rangle$. By then measuring the first system (in the orthonormal $|\alpha_i\rangle$ basis), Alice is preparing the signal states $|\phi_i\rangle$ with probabilities p_i. By pretending that their data comes from the equivalent two photon state, Alice and Bob should be able to use their data to prove entanglement.

continuous degrees of freedom (e.g., quadratures or time and frequency) rather than polarization, a single photon can carry more information than just one (qu)bit. An example especially relevant to our discussion—it in fact formed the inspiration for this work—is the possibility of encoding and decoding multiple bits of information in the time and frequency degrees of freedom of pairs of photons, as discussed in Ref. [25] (see also [45]). An important ingredient of that work is a scheme for converting the time measurement into a much more precise frequency measurement, at the cost of losing some flexibility in choosing the range of detection.

In every entanglement verification or quantum cryptography experiment one has to deal with missing data due to imperfect detectors. For missed counts *inside* the detector range we typically assume that the missing data would follow the same statistics as the recorded data. (When Bell inequalities are used to eliminate or refute hidden-variable theories, no such assumption may be used. Imperfect detectors then lead to the so-called detection loophole. But when using the same Bell inequalities for entanglement verification the assumption is typically warranted [19].) Here, in contrast, we worry about missed counts from *outside* one's detector range. The assumption that those counts would follow the same statistics as the recorded data is meaningless. We will show that exactly how one should take into account missing data of this type depends on what criterion one uses to verify entanglement (or to prove cryptographic security) .

4.2. Detecting continuous-variable entanglement

4.2.1. Entanglement criteria

The best known and easiest to calculate separability criterion developed for detecting discrete variable bipartite entanglement is the positive partial transpose

(PPT) criterion [27]. The PPT criterion has been extended to bipartite CV systems by Shchukin and Vogel [46] and by Miranowicz *et al.* [47], which encompasses previous CV criteria by Duan *et al.* [48], Simon[49], Raymer *et al.*[50], Mancini *et al.*[51], and others. For example the Mancini-Giovanetti-Vitali-Tombesi (MGVT) criterion states that if $U_- = u_a - u_b$ and $V_+ = v_a + v_b$, where u and v are some dimensionless scaled variables for particles a and b, with $[u_j, v_{j'}] = i\delta_{j,j'}$ $(j, j' = a, b)$ then for all separable states the variances of U_- and V_+ satisfy

$$\sigma^2[U_-]\sigma^2[V_+] \geq 1. \tag{4.1}$$

Violation of this condition on variances means that the underlying state is verifiably entangled.

In experiments on down conversion photons are created in pairs, such that the two photons are correlated in time (the two photons are created at the same time by annihilation of a high-energy photon, up to a small difference in time allowed by the time-energy uncertainty relation) but anti-correlated in frequency (because of energy conservation, with imperfect anti-correlations arising from uncertainty in the initial photon's frequency). So, in our intended application, U_- would be taken to be the difference in detected times-of-arrival and V_+ would be the sum of the detected frequencies.

4.2.2. Coarse grained measurements

To use the criterion of Eq. (4.1) to verify continuous variable entanglement of a state using experimental data, one must take into account how the detectors are used to measure the observables $\hat{u}$ and $\hat{v}$, and possibly modify the criterion

accordingly. The first thing that must be considered is the coarse grained nature of the measurements. While the variable being measured is continuous, our detectors have finite resolution and our data is binned. Instead of measuring $\hat{u}$ and $\hat{v}$ we are measuring the observables

$$\hat{u}^{\Delta} = \sum_{k=1}^{D} \int_{u_k-\Delta/2}^{u_k+\Delta/2} du\, u_k |u\rangle\langle u|, \tag{4.2}$$

$$\hat{v}^{\delta} = \sum_{l=1}^{D} \int_{v_l-\delta/2}^{v_l+\delta/2} dv\, v_l |v\rangle\langle v|, \tag{4.3}$$

where $u_k = (k - D/2)\Delta + u_0$ and $v_l = (l - D/2)\delta + v_0$, and where Δ and δ are the resolutions of the u and v detectors, respectively. We assumed here, for simplicity, the number of bins, D, to be the same for u and v measurements. The variances we need to calculate are now given by

$$\begin{aligned} \sigma^2[U_-^{\Delta}] &= \langle(\hat{u}_a^{\Delta} - \hat{u}_b^{\Delta})^2\rangle - \langle(\hat{u}_a^{\Delta} - \hat{u}_b^{\Delta})\rangle^2, \\ \sigma^2[V_+^{\delta}] &= \langle(\hat{v}_a^{\delta} + \hat{v}_b^{\delta})^2\rangle - \langle(\hat{v}_a^{\delta} + \hat{v}_b^{\delta})\rangle^2, \end{aligned} \tag{4.4}$$

Tasca *et al.* [52] modified the MGVT criterion for coarse grained measurements and showed all separable states satisfy [52]

$$\left(\sigma^2[U_-^{\Delta}] + \frac{\Delta^2}{12}\right)\left(\sigma^2[V_+^{\delta}] + \frac{\delta^2}{12}\right) \geq 1, \tag{4.5}$$

and so a violation of this inequality proves entanglement. This condition is harder to violate than (4.1) because of the presence of the extra bin width dependent terms on the left hand side. That is, the binning of the data loses information, and makes it harder to verify entanglement. Although it is not clear from Ref. [52] to what

variables this criterion is meant to be applied, we will proceed using this criterion with the variances as we have defined in Eq. (4.4) as an example since our purpose ultimately is not to suggest this (or any other variance based criteria) as a method to verify entanglement. Rather, we aim to show that *any* variance based criteria is not well suited for entanglement verification when taking into account the finite range of the detectors, even if one were to overestimate the entanglement by ignoring the binning of data completely.

4.2.3. Finite range detectors

The correction for coarse graining alone is not sufficient to properly verify entanglement experimentally. An additional correction must be made to take into account the finite detection range of the detectors. In general the wavefunction is not zero outside the detection range, so there is some probability of "missed counts"—events that occur when the particle arrives at the detector but is not detected because it falls outside the detection range. (This is different than not being detected because of transmission loss or detector inefficiency.)

To illustrate the importance of being earnest about the missed counts, let us first consider a pure *separable* gaussian bipartite state, shared between Alice and Bob, of the form

$$\Psi(v_a, v_b) \propto \exp\left(\frac{-v_a^2}{2s^2}\right) \exp\left(\frac{-v_b^2}{2s^2}\right), \tag{4.6}$$

with s chosen such that the particles' wavefunction is well localized in the variables v_a and v_b. Hence, the value of V_+^δ is quite sharply defined, but, as a consequence, the probability distribution for the complementary variables u_a and u_b is broad and U_-^Δ is not sharply defined. For simplicity we will assume in our examples that Alice and Bob are using detectors of the same resolution and range for both $u_{a,b}$ and $v_{a,b}$.

Since the probability distribution in $u_{a,b}$ extends well beyond their detection range, the probability of Alice and Bob both detecting a particle when measuring in the $u_{a,b}$ basis will be small. For, e.g., $s = 1/8$ and a detection range of $[-2, 2]$ this probability is only about 7.6%, whereas in the $v_{a,b}$ basis it is essentially 100%. From now on, we always fix Alice's and Bob's detector ranges to $[-2, 2]$(with the exception of Figure 4.4. below, where we study the effect of varying the detector range).

Now consider a mixed state consisting of a 50/50 mixture of the separable state we just examined and a similar separable state equally sharply peaked in u_a and u_b. This mixed state will have sharp features in both u and v, while most of the broad background distribution falls outside the detection window. The probability of detecting both particles is only 53.8% for either basis. Ignoring the missed counts, U_-^Δ and V_+^δ are mostly sharply defined, and look similar to what the results would be for an entangled EPR-like state. After measuring the state with 32 bin resolution detectors, naively normalizing the detected data to 100% as in Figure 4.1., and calculating $(\sigma^2[V_+^\delta] + \frac{\delta^2}{12})(\sigma^2[U_-^\Delta] + \frac{\Delta^2}{12}) \approx .04 < 1$, the coarse grained MGVT criterion will "verify entanglement" even though the underlying state clearly is separable.

4.3. Worst-case analysis

4.3.1. Assumptions

The preceding example shows we must account for the missed data in some way. To do this we assume that we know what percentage of counts are missed (this information could be obtained by using a detector of lower resolution but much broader range). We also assume that we can set a cutoff beyond which counts can be ignored. We return to this cutoff assumption below in Sec. 4.3.5.

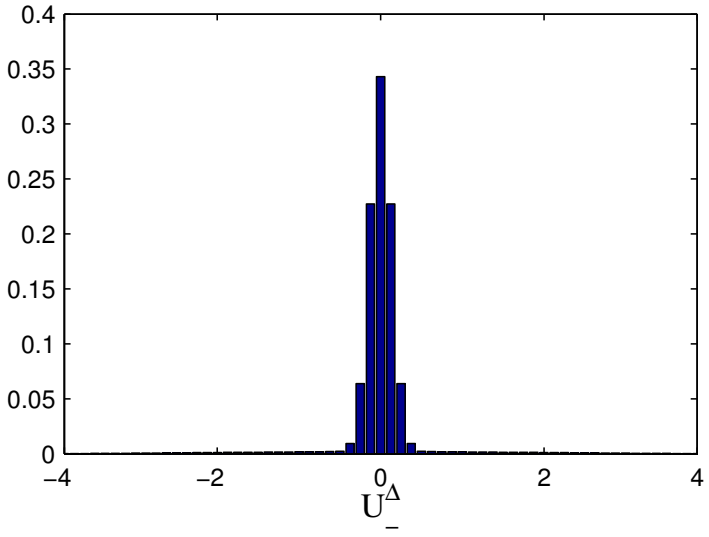

FIGURE 4.1. U_-^Δ for mixed separable state, where the missed counts outside the detector range have been ignored (the graph for V_+^δ would look identical). We would falsely conclude we have entanglement. Note the barely visible background level of counts: in order to properly reach conclusions about entanglement, we would need to know how far those background counts extend outside our detector range.

For our worst-case analysis we add additional bins to U_-^Δ and V_+^δ that correspond to values that could have been measured outside our detector range, but inside the our cutoff. In order to properly verify entanglement we must then add the missed counts to our data in the worst way possible so that we will not be led to believe that we have entanglement (or security) when we do not. For the MGVT criterion this means we should maximize the variance of U_-^Δ and V_+^δ, and so we add the missed counts to the outermost bins of U_-^Δ and V_+^δ (the weighting depends on the experimental data and the cutoffs. For symmetric experimental data and symmetric cutoffs, half of the missed counts goes into each of the outermost bins, as depicted in Figure 4.2.a). To attempt to verify entanglement for the mixed separable state example, we find that by setting cutoffs at, say, -40 and 40 for the detectors of both Bob and Alice, they would fail to both detect particles less than 10^{-9} percent of the time. The choice of

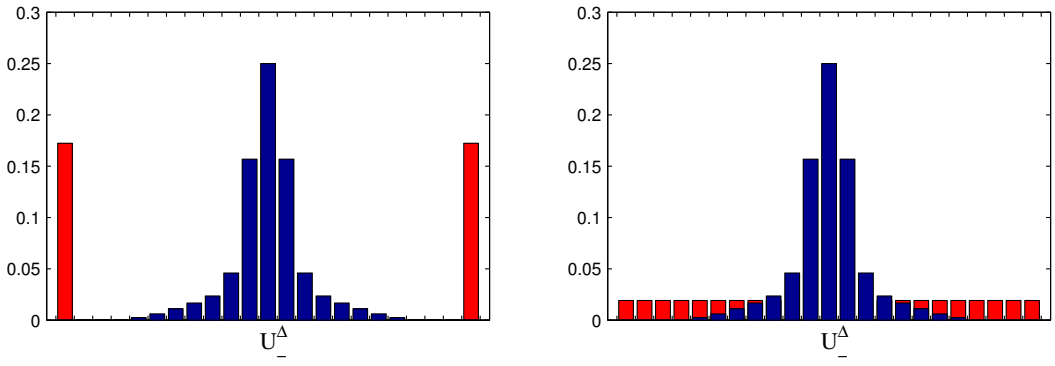

FIGURE 4.2. Left: Cartoon showing how to deal with missing data (red) outside our detector range for a *variance*-based entanglement or security criterion. After having determined a cutoff range beyond which we expect no counts, missed data are assigned to the outside bins within the cutoff range. Right: Same for an *entropic* entanglement or security criterion: missed data are as uniformly distributed as possible within the cutoff range.

cutoff corresponds to adding 1216 bins for U_-^Δ and V_+^δ, in the outermost of which we place the missing data. The variances increase so much that we no longer come close to concluding that we have entanglement.

4.3.2. Smoothed EPR state

Because of the necessity of adding the missing data in the worst way and the strong dependence of the variance on the cutoff and amount of missed counts, the MGVT criterion will often fail to detect entanglement when it is, in fact, present. For example, consider an *entangled* gaussian state ("smoothed EPR" [53])

$$\Psi(u_a, u_b) \propto \exp\left(2\sqrt{\bar{n}(\bar{n}+1)}u_a u_b - (\bar{n}+\frac{1}{2})(u_a^2+u_b^2)\right), \tag{4.7}$$

where for $\bar{n}=0$ the state is separable and in the limit $\bar{n}\to\infty$ we have the original EPR state. For $\bar{n}=1$ and a detection range of $[-2,2]$ (see Figure 4.3.a) the probability

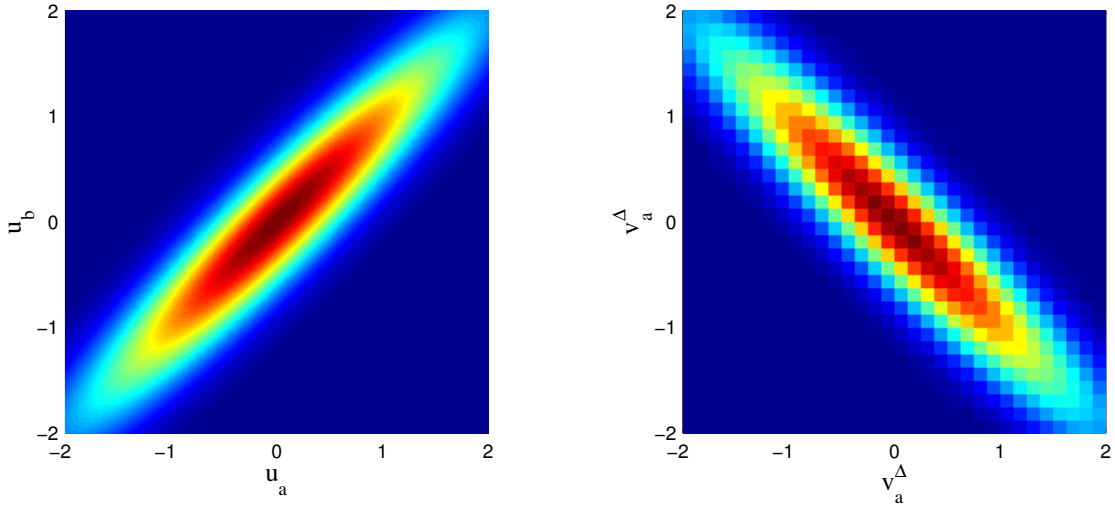

FIGURE 4.3. Left: $|\Psi(u_a, u_b)|^2$ for the smoothed EPR state (4.7) with $\bar{n} = 1$; Right: $|\Psi(v_a, v_b)|^2$ for the same smoothed EPR state as measured by detectors with a 32 bin resolution

of both parties detecting a particle is about 86.9% For this case, without even adding extra bins to U_-^Δ and V_+^δ and simply putting the missing data into the outermost of the existing bins inside the detector range, we already fail to verify the entanglement present in the state with the modified MGVT criterion, no matter what the cutoff would be. Other variance-based criteria fare equally badly.

4.3.3. Renyi entropies

A better choice is to use a criterion that does not depend as strongly on the location of the cutoff or the probability of missed counts. Instead of using a variance-based criterion we will now look at an entropic criterion. Continuous variable separability criteria have been developed using Shannon, Tsallis, smooth and Renyi entropies [54–56]. We focus on Renyi entropies here, but will return to

smooth entropies in Sec. 4.3.6. The Renyi entropy of order α for a binned probability distribution is defined as

$$H_\alpha[B^{\delta b}] = \frac{1}{1-\alpha} \ln(\sum_k (B_k^{\delta b})^\alpha). \tag{4.8}$$

By following a proof of a separability criterion given in [55] for unbinned joint variables, and then inserting the uncertainty relations derived in [57] for binned variables, we obtain this inequality

$$H_\alpha[U_-^\Delta] + H_\beta[V_+^\delta] + \frac{1}{2}\left(\frac{\ln\alpha}{1-\alpha} + \frac{\ln\beta}{1-\beta}\right) - \ln\frac{2\pi}{\Delta\delta} \geq 0, \tag{4.9}$$

for $1/\alpha + 1/\beta = 2$, which is satisfied for any separable state. So if this equality is violated for *any* such constrained pair of values α and β, the underlying state is verifiably entangled. The criterion is optimized by minimizing the left-hand side over the allowed values for α, β. The inequality (4.9) has the same form as Eq. (26) of Ref. [55], but our inequality applies to the measurable binned observables (where Alice and Bob bin their data, and then take the difference/sum of the binned outcomes), whereas Eq. (26) of Ref. [55] applies to observables obtained by first taking the difference/sum and then binning.

To deal with the missed counts when using this criterion we again add additional bins to U_-^Δ and V_+^δ that correspond to values that could have been measured outside our detector range, but inside a cutoff. We then must add the missing data such that it maximizes the Renyi entropy. Since the Renyi entropy is maximized by a uniform distribution, we will add the missed counts to the new empty bins and the existing bins with few counts to make the distribution as uniform as possible, as

shown in cartoon form in Figure 4.2.b We then optimize our criterion and hope we verify entanglement.

4.3.4. Numerical examples

For a smoothed EPR state with $\bar{n} = 1$, Alice and Bob would only fail to both detect a particle less than 10^{-12} percent of the time in the range $[-10, 10]$, so they could choose that as their cutoff range (adding those missed counts to the region beyond the cutoff would make a negligible contribution). They add 256 bins to U_-^Δ and V_+^δ and distribute the missing data in the most uniform way possible. After doing this and optimizing the criterion, they do indeed verify entanglement. (Recall that the variance criterion *always* fails for this case.) The Renyi entropy criterion depends

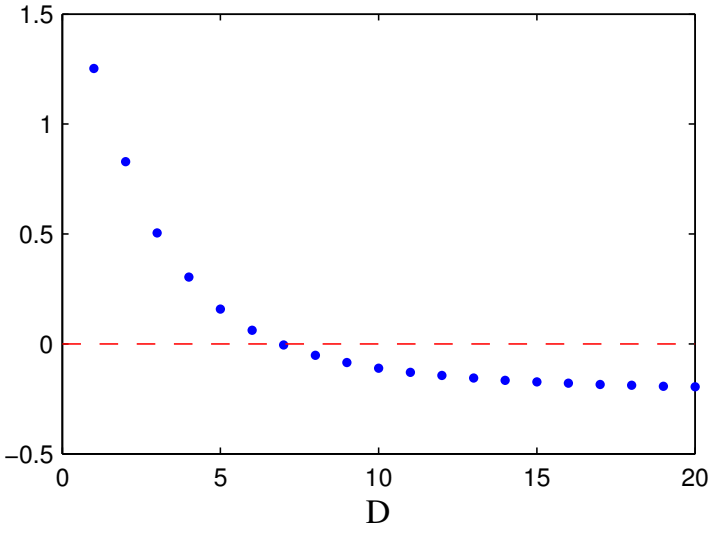

FIGURE 4.4. Optimized Renyi criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the number of bins inside the detection range. One needs a minimum number of 7 bins to verify entanglement.

on the size of the bins both in the explicit bin width term and the Renyi entropy terms. Fixing the detection range and cutoff, and varying the number of bins D of

our detectors, we see in Figure 4.4. that in this instance entanglement will be verified if we include at least 7 bins. If we have fewer bins, we throw too much information away and can not be sure we have entanglement.

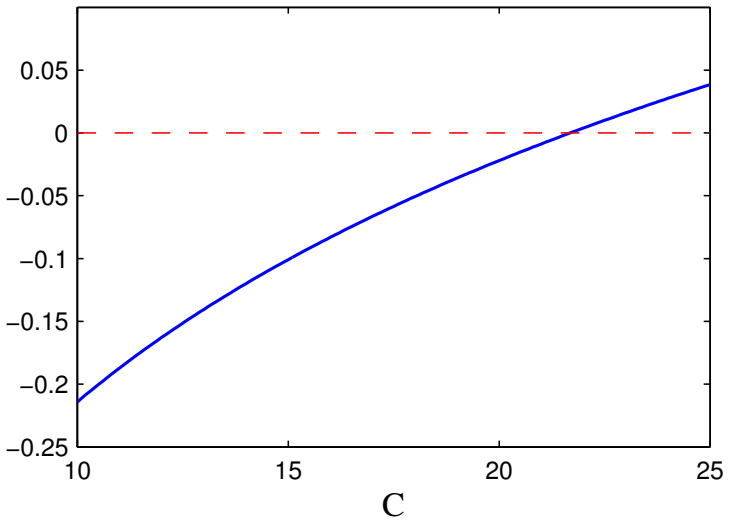

FIGURE 4.5. Optimized criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the detection cutoff C, which assumes no detection events would occur outside the interval $[-C, C]$). One needs $C < 21.5$ in order to be able to verify entanglement.

The strength of the Renyi entropy criterion is its smaller sensitivity to the location of the cutoff. In Figure 4.5. we see that entanglement will be verified for the $\bar{n} = 1$ smoothed EPR state as long as the cutoff range does not exceed $[-21.5, 21.5]$.

One might also wonder how the ability to verify entanglement depends on the detection range. Figure 4.6. shows that, for a fixed outer cutoff of [-10,10], entanglement will be verified if the detector range is larger than [-1.9,1.9]. For ranges smaller than this, there is too much missing data that has to be distributed in the worst way possible.

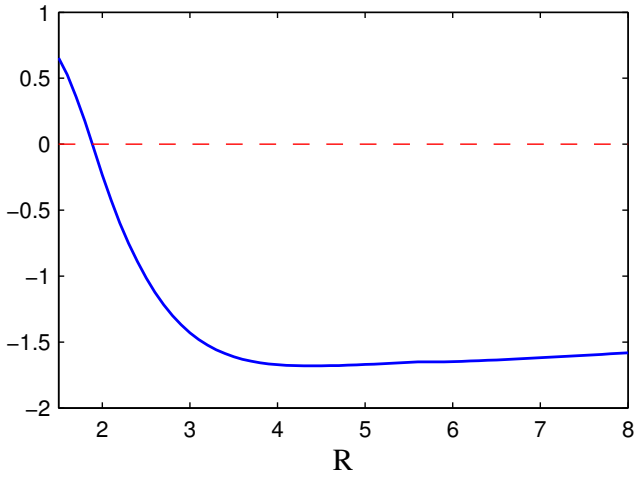

FIGURE 4.6. Optimized criterion, N, for the smoothed EPR state with $\bar{n} = 1$ as a function of the detector range $[-R, R]$ with a fixed outer cutoff of [-10,10]. Entanglement can only be verified when the detection range is larger than [-1.9,1.9].

4.3.5. The cutoff assumption

In order to obtain a finite estimate of a variance, we need to assume that there is a cutoff beyond which detections can be safely ignored. This is, in fact, what one always has to assume in any physics experiment that measures some in principle unbounded quantity. Namely, consider an experiment measuring some observable X. If even with a tiny probability $p(X)$ a very large value could occur, then our reported average value $\bar{X}$ could be unreliable. Obviously, if $p(X)$ decays sufficiently fast with $|X|$ then the effect of outliers on the average value will be negligible. But at the same time (for instance, if $p(X) \propto 1/|X|^2$) the effect on the variance in our estimate could still be substantial. We have assumed here that $p(X)$ decays sufficiently fast outside the cutoff region so as not to affect our estimate of the variance. *A fortiori*, it affects our estimate of the entropy even less. This is one more reason to use entropic criteria for verifying entanglement of continuous-variable states, or to test security in continuous-variable protocols.

We also note that these considerations are in addition to the fact that a finite experiment can only ever reach a probabilistic statement about entanglement. For a discussion on how to quantify probabilistic evidence for entanglement in a finite experiment, see [30].

Finally, we note that our assumption of a finite detector range within the cutoff range is motivated by an actual experimental setup [25], in which there is a tradeoff between number of bins, their width, and the accuracy of detections in a given bin. In an ideal world, the cutoff would be set equal to the detection range.

4.3.6. Smooth entropies

For our entropic entanglement criterion we used an inequality based on the Renyi entropy, since a nice and relatively simple necessary criterion for separability exists, which in addition takes into account the binning of data [55]. But there are alternatives. In particular, recent work on "smooth entropies" has shown that optimal uncertainty relations can be obtained [56, 58], and that these relations can be used to prove security of a continuous-variable quantum key distribution protocol [59]. In principle, smooth entropies could be used for our purposes, too, and would, possibly, lead to better criteria. For instance, in Ref. [59] the assumption of a cutoff was not necessary. On the other hand, there one did make an assumption about the form of the state, namely that it is a two-mode squeezed state. Much more complicated maximizations would have to be performed to obtain state-independent bounds, and it is not clear whether such bounds can be obtained without in the end resorting to standard von Neumann entropies.

4.4. Conclusions

We discussed a difficulty that arises in entanglement verification (or quantum cryptography) experiments for continuous variable systems, which does not seem to have been discussed in the literature yet: missing data *outside* one's detector range. We showed how to take those missing data into account, by distributing them over the outside range in the worst possible way, given the criterion one uses to verify entanglement (or prove security), as schematically pictured in Figures 4.2.a and 4.2.b As a consequence, entropic entanglement (security) criteria turn out to be much more forgiving than are variance-based criteria (including the well-known Duan-Simon entanglement criteria).

We investigated mainly one criterion, which takes into account the binning of data and is based on the Renyi entropy, but other criteria are worth investigating, too: we mentioned smooth entropies [56, 58], and the Vogel-Shchukin [46] method of moments looks promising as it, too, can take into account the binning of data.

In this chapter we discussed the general case of verifying continuous variable entanglement and issues arising from performing measurements with detectors of finite range. In the next chapter we will examine a specific case of interest motivated by a recently proposed QKD scheme using time-frequency entangled photon pairs [25].

CHAPTER V

MISSING DATA OUTSIDE THE DETECTOR RANGE: APPLICATION TO TIME-FREQUENCY ENTANGLEMENT

This work has been submitted for publication in Physical Review A. It was initiated by S. J. van Enk and finished jointly by Megan R. Ray and S. J. van Enk.

5.1. Introduction

Time-frequency entangled photon pairs have recently become of interest for QKD schemes due to their large information capacity (i.e. multiple bits per photon), ease of preparation, and robustness against transmission noise [25, 60–62].

One previously proposed QKD protocol [63] used the time and frequency bases for encoding information by using single photons (not entangled) with a prepare-and-measure method. Here Alice randomly and controllably modulates either the frequency or time delay (relative to a reference pulse) of a single photon that is sent to Bob, who then randomly chooses to measure in either the time or frequency basis. The required random and controlled modulation is difficult, making the protocol somewhat impractical. Additionally, the density matrix of the photon sent to Bob will in practice depend on the basis that Alice prepares in, possibly allowing an eavesdropper to distinguish between preparation bases thereby compromising security. An alternative to the single-photon prepare-and-measure method is to use time-frequency entangled photon pairs, whose measurement results are naturally correlated. Moreover, the density matrix of the photon propagating to Bob is guaranteed to be independent of the basis Alice performs her measurement in.

Spontaneous parametric down conversion (SPDC) and four wave mixing (FWM) are well-known and established sources of time-frequency entangled photon pairs with highly tailorable spectral/correlation properties [64–66]. In SPDC a pump photon with frequency ω_p traveling through a nonlinear crystal will, with some small probability, be annihilated and simultaneously two (entangled) photons will be created with frequencies ω_A and ω_B [67]. Conservation of energy results in the downconverted pair being anti-correlated in frequency, since $\omega_p = \omega_A + \omega_B$ to within the bandwidth of the original pump photon. Because they are created at the same time, the time of arrival of the two photons will be correlated. Similarly, in the FWM process two photons, with frequencies ω_1 and ω_2, propagating in a non-linear material (e.g. a photonic crystal fiber) are annihilated and at the same time two photons with different frequencies, ω_A and ω_B, are created [68], leading again to an entangled photon pair that is correlated in time and anti-correlated in frequency $(\omega_1 + \omega_2 \approx \omega_A + \omega_B)$.

While there has been theoretical interest in entangled time-frequency QKD protocols, this has not yet been experimentally demonstrated[1]. The technical challenge in implementing an entangled time-frequency QKD protocol has been in the ability to perform the measurements that would be required. It has not been possible to perform measurements in both the time and frequency bases with sufficient resolution and efficiency at the single photon level with current spectrometers and time-resolving photodetectors, since high resolution detectors tend to be inefficient, and since a broad spectral profile implies a narrow temporal profile, and vice versa.

A way around this problem was recently proposed in [25]. By performing time to frequency (T2F) conversion, one can map the temporal profile of a photon

[1]Such states were used in a non-standard QKD protocol [69] which encoded only in a single (temporal) basis. It's not clear whether such a protocol is secure.

to the frequency domain and then measure it with a spectrometer, allowing for higher temporal resolution than could be obtained with a direct time measurement. By implementing this technique, the authors of Ref. [25] believe that 4 bits per photons would be achievable with currently available off the shelf components, and larger alphabets would be possible in the future as the technologies used in the T2F conversion improve. We will examine the ability to verify time-frequency entanglement for the proposed system using the methods of the previous chapter.

5.2. Measurements

In each trial (that is, for each photon pair produced by the source) Alice and Bob randomly and independently measure either the frequency or time of arrival of their photon. We assume they have identical measurement devices, described below. They perform many trials, a relatively small number of which will be used to evaluate security (by verifying entanglement) and the rest of which will be used to ultimately generate the secret key.

5.2.1. Frequency measurements

Alice and Bob measure in the frequency basis using photon counting spectrometers. Each of their detectors have D bins of width $\delta\omega$, giving a detection range of $\Delta\omega = D\delta\omega$. The measurement is modeled in the same way as in the previous chapter:

$$\hat{\omega}^{\delta\omega} = \sum_{k=1}^{D} \int_{\omega_k-\delta\omega/2}^{\omega_k+\delta\omega/2} \mathrm{d}\omega\, \omega_k |\omega\rangle\langle\omega|, \tag{5.1}$$

where $\omega_k = (k - D/2)\delta\omega + \omega_0$ is the central frequency of the kth bin.

5.2.2. Time measurements (using time to frequency conversion)

Rather than making direct time measurements, Alice and Bob each achieve a high resolution time measurement by performing T2F conversion on their photon before measuring frequency. The T2F conversion, as described in Refs.[70–73], is implemented by passing the photon through a dispersive delay line (DDL) and an electro-optic phase modulator (EOM). To see how this affects our state, we start with a pure single-photon state described by

$$\left|\tilde{\Psi}\right\rangle = \int \mathrm{d}t\, \tilde{f}(t)\, |t\rangle\,, \tag{5.2}$$

where $|t\rangle = (2\pi)^{-1/2} \int \mathrm{d}\omega\; a^{\dagger}(\omega) \exp(-i\omega t)\, |\mathrm{vac}\rangle$ and $\tilde{f}(t)$ is normalized to $\int \mathrm{d}t |\tilde{f}(t)|^2 = 1$. The DDL (which can simply be an ordinary silica fiber) acts in the frequency domain as a multiplication by a frequency dependent phase factor $G(\omega) = \exp(i\varphi(\omega))$, with $\varphi(\omega) = \ddot{\varphi}\omega^2/2$, where $\ddot{\varphi}$ is the group velocity dispersion of the fiber, a constant dependent on the length of the fiber, so that

$$f(\omega) \rightarrow G(w) f(\omega) = \exp[\frac{i}{2}\ddot{\varphi}\omega^2] f(\omega). \tag{5.3}$$

This transformation can be expressed in the time domain as a convolution

$$\begin{aligned} \tilde{f}(t) \rightarrow (\tilde{G} * \tilde{f})(t') &= \frac{1}{\sqrt{-i\ddot{\varphi}}} \int \mathrm{d}t \exp[\frac{-i}{2\ddot{\varphi}}(t-t')^2] \tilde{f}(t) \\ &= \frac{1}{\sqrt{-i\ddot{\varphi}}} \exp[\frac{-i}{2\ddot{\varphi}} t'^2] \int \mathrm{d}t \exp[\frac{-i}{2\ddot{\varphi}} t^2] \exp[\frac{i}{\ddot{\varphi}} t t'] \tilde{f}(t). \end{aligned} \tag{5.4}$$

The EOM acts as multiplication by a time-dependent phase factor $\tilde{H}(t) = \exp(i\phi(t))$, with a phase $\phi(t) \cong \ddot{\phi} t^2/2$ near the peak modulation ($t \approx 0$), where $\ddot{\phi}$ is a constant

related to the modulation depth. The modulation frequency must be chosen such that the approximation $\phi(t) \cong \ddot{\phi}t^2/2$ is valid for the full duration of the signal. This dictates the resolution that is achievable, as discussed in [25]. Advances in modulator technology should allow for higher resolution measurements and thus a larger alphabet. The combination of the two transformations yields

$$\begin{aligned}(\tilde{G} * \tilde{f})(t') \rightarrow & \tilde{H}(t')(\tilde{G} * \tilde{f})(t') \\ & = \exp[\frac{i}{2}\ddot{\phi}t'^2](\tilde{G} * \tilde{f})(t') \\ & = \frac{1}{\sqrt{-i\ddot{\varphi}}} \exp[\frac{i}{2}t'^2(\ddot{\phi} - \frac{1}{\ddot{\varphi}})] \int \mathrm{d}t \exp[\frac{-i}{2\ddot{\varphi}}t^2] \exp[\frac{i}{\ddot{\varphi}}tt']\tilde{f}(t). \end{aligned} \tag{5.5}$$

If the DDL and EOM parameters are chosen such that $\ddot{\phi}\ddot{\varphi} = 1$, the state that results after applying both the DDL and EOM is

$$\frac{1}{\sqrt{-i\ddot{\varphi}}} \int \mathrm{d}t \ \exp[\frac{-i}{2\ddot{\varphi}}t^2] \exp[\frac{i}{\ddot{\varphi}}tt']\tilde{f}(t). \tag{5.6}$$

The Fourier transform of this state can be evaluated as follows:

$$\begin{aligned} & \frac{1}{2\pi\sqrt{-i\ddot{\varphi}}} \int \int \mathrm{d}t' \mathrm{d}t \ \exp[i\omega t] \exp[\frac{-i}{2\ddot{\varphi}}t^2] \exp[\frac{i}{\ddot{\varphi}}tt']\tilde{f}(t) \\ & = \frac{1}{\sqrt{-i\ddot{\varphi}}} \int \mathrm{d}t \ \exp[\frac{-i}{2\ddot{\varphi}}t^2]\tilde{f}(t)\delta(\omega - \frac{t}{\ddot{\varphi}}) \\ & = \frac{1}{\sqrt{-i\ddot{\varphi}}} \tilde{f}(\ddot{\varphi}\omega) \exp[\frac{-i\ddot{\varphi}}{2}\omega^2]. \end{aligned} \tag{5.7}$$

So we see when the DDL and EOM are chosen such that $\ddot{\phi}\ddot{\varphi} = 1$, their combined action is to produce a Fourier transform of the original state, up to a scaling and frequency dependent phase factor.

After the T2F conversion, the state is measured with the same type of photon counting spectrometer described above. The resolution of this measurement is $\delta t = \ddot{\varphi}\delta\omega = \delta\omega/\ddot{\phi}$ and the range is $\Delta t = D\delta t = D\delta\omega/\ddot{\phi} = \Delta\omega/\ddot{\phi}$.

5.2.3. Cutoff and missing data

As discussed in the preceding chapter, Alice and Bob must also make measurements to determine an appropriate cutoff and how much data they are missing. This can be done with spectrometers with a larger range but lower resolution.

5.3. Verifying entanglement

After completing many trials, Alice and Bob publicly announce their measurement bases for each trial. After discarding measurements for trials when they measured in different bases or when they failed to both detect a photon, they randomly choose a subset of measurements that will be used to verify entanglement. We will use a Renyi entropy criterion of the type discussed in the last chapter. The continuous operators useful for verifying time-frequency entanglement with such a criterion for states correlated in time and anti-correlated in frequency are

$$\hat{\Omega}_+ = \hat{\omega}_A + \hat{\omega}_B, \tag{5.8}$$

$$\hat{T}_- = \hat{t}_A - \hat{t}_B. \tag{5.9}$$

The discrete approximations of these, based on the measurements that Alice and Bob make, are

$$\Omega_+^{\delta\omega} = \hat{\omega}_A^{\delta\omega} + \hat{\omega}_B^{\delta\omega} \tag{5.10}$$

$$T_-^{\delta t} = \hat{t}_A^{\delta t} - \hat{t}_B^{\delta t} \tag{5.11}$$

As we saw in the last chapter, all separable states must satisfy

$$H_\alpha[T_-^{\delta t}] + H_\beta[\Omega_+^{\delta\omega}] + \frac{1}{2}\left(\frac{\ln\alpha}{1-\alpha} + \frac{\ln\beta}{1-\beta}\right) - \ln\frac{2\pi}{\delta\omega\delta t} \geq 0, \tag{5.12}$$

for any α, β chosen such that $1/\alpha + 1/\beta = 2$. In the same way as in the last chapter, we will denote the l.h.s of Eq.(5.12), minimized over the constrained values of α and β, by M:

$$M := \min_{\alpha,\beta:1/\alpha+1/\beta=2} H_\alpha[T_-^{\delta t}] + H_\beta[\Omega_+^{\delta\omega}] + \frac{1}{2}\left(\frac{\ln\alpha}{1-\alpha} + \frac{\ln\beta}{1-\beta}\right) - \ln\frac{2\pi}{\delta\omega\delta t}. \tag{5.13}$$

Then we can say that if $M < 0$ the state is verifiably entangled.

After adding the missing data in the worst way possible (i.e. the way that makes the distribution most uniform) Alice and Bob can calculate M and hope that it is less than 0. If it is not, they abort the protocol and start again, since they cannot be sure there is no eavesdropper.

5.4. Ideal state

A general pure two-photon state, with the two photon frequencies written as $\omega_A + \omega_0$ and $\omega_B + \omega_0$ (where ω_0 is central frequency of the pair), can be described by

$$|\Psi\rangle = \iint \mathrm{d}\omega_A \, \mathrm{d}\omega_B \; f(\omega_A, \omega_B) \, |\omega_A, \omega_B\rangle \,, \tag{5.14}$$

where

$$|\omega_A, \omega_B\rangle = a^\dagger(\omega_A) a^\dagger(\omega_B) \, |\mathrm{vac}\rangle \tag{5.15}$$

and the joint spectral amplitude, $f(\omega_A, \omega_B)$, can be chosen symmetric in its two arguments without loss of generality, and is normalized as $\int\int \mathrm{d}\omega_A \mathrm{d}\omega_A \, |f(\omega_A, \omega_B)|^2 = 1$. The central frequency for a SPDC process is $\omega_0 = \omega_p/2$, and for FWM it is $\omega_0 = (\omega_1 + \omega_2)/2$.

The particular form of f proposed and analyzed in [25] is an idealized version of the time-frequency entangled state resulting from FWM or SPDC [67, 74]:

$$f(\omega_A, \omega_B) = (\pi \Lambda_+ \Lambda_-)^{-1/2} \exp\left(-\omega_-^2/2\Lambda_+^2 - \omega_+^2/2\Lambda_-^2\right), \tag{5.16}$$

where $\omega_\pm = (\omega_A \pm \omega_B)/\sqrt{2}$ and Λ_+, Λ_- are the marginal and correlation bandwidths, respectively. It is convenient to define these in terms of the bin width and detection range of the spectrometers: $\Lambda_- = \beta_- \delta\omega$ and $\Lambda_+ = \beta_+ \Delta\omega$. The joint temporal amplitude corresponding to Equation (5.16) is

$$\tilde{f}(t_A, t_B) = (\pi \sigma_+ \sigma_-)^{-1/2} \exp\left(-t_-^2/2\sigma_-^2 - t_+^2/2\sigma_+^2\right), \tag{5.17}$$

where $\sigma_+ = 1/\Lambda_-$ and $\sigma_- = 1/\Lambda_+$ and $t_\pm = (t_A \pm t_B)/\sqrt{2}$. The T2F setup is designed such that the resolution of the time correlation matches that of the frequency measurement, that is $\ddot{\phi}$ is chosen to be $\ddot{\phi} = \delta\omega/\delta t = \beta_-\beta_+\delta\omega^2 D$ so that $\delta t = \sigma_-/\beta_-$.

For an experimentally feasible QKD system based on currently available technology, the authors of [25] propose using spectrometers composed of 16 bins of 2nm width in the telecom region, and engineering their state so that $\beta_+ = 3/4$ (this provides a somewhat uniform detection probability amongst the detection channels) and $\beta_- = 1/5$ (this provides strong enough correlation that $\Omega_+^{\delta\omega}$ and $T_-^{\delta t}$ are mostly confined to one bin). Figure 5.1. shows the continuous joint spectral probability distribution, $|f(\omega_A, \omega_B)|^2$, and the binned joint temporal probability distribution, $|\tilde{f}(t_A, t_B)|^2$, for the state with these parameters.

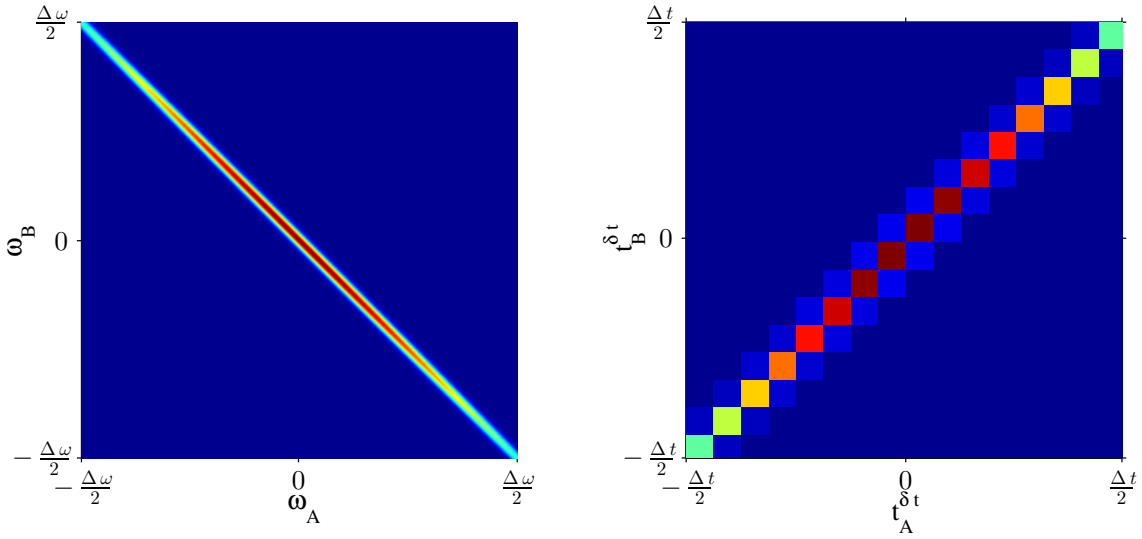

FIGURE 5.1. Left: Continuous joint spectral probability, $|f(\omega_A, \omega_B)|^2$ for parameters specified in [25] Right: Binned joint temporal probability, $|\tilde{f}(t_A, t_B)|^2$, as measured with detectors with D=16 bins.

The disadvantage in choosing β_+ such that the detection probability amongst the detection channels is somewhat uniform (as seen in Figure 5.2.) is that the probability of not detecting the photons because they fall outside the range of the detector becomes significant. For the choices of parameters given above, the probability of both Alice and Bob detecting photons when measuring in the same basis is about 81%, which means that about 19% of the data is missing and will need to be distributed in the worst way possible, making it harder (less likely) to verify entanglement

We see in Figure 5.3. that entanglement will be verified as long as the cutoffs are chosen to be less than $[-4.8(\frac{\Delta}{2}), 4.8(\frac{\Delta}{2})]$, $(\Delta = \Delta\omega, \Delta t)$. We will choose for concreteness to use cutoff ranges $[-3.5(\frac{\Delta}{2}), 3.5(\frac{\Delta}{2})]$ for both $\Delta\omega$ and Δt, which correspond to one or both parties failing to detect a photon with a probability of order 10^{-6} when measuring in the same basis.

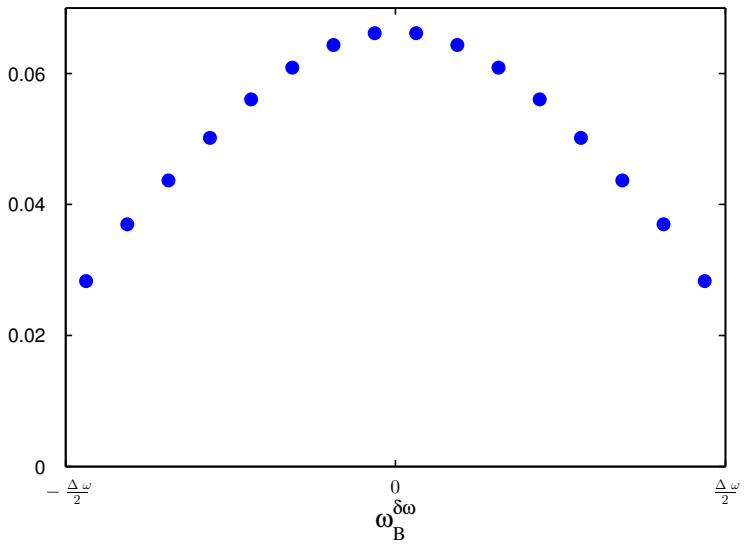

FIGURE 5.2. Probability of detection for each bin of Bob's detector for parameters specified in [25], conditioned on Alice also detecting a photon. $\beta_+ = 3/4$ was chosen such that this is "reasonably flat"[25].

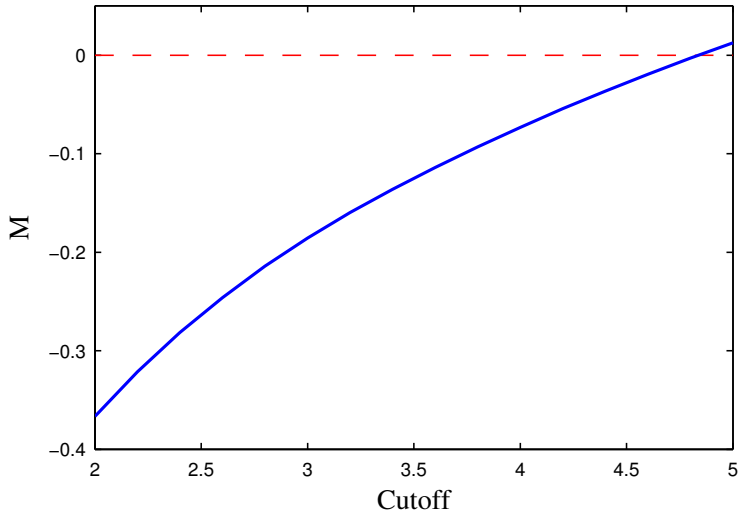

FIGURE 5.3. Optimized entanglement criteria, M, as a function of the outer cutoff, where the outer cutoff in units of $\Delta/2$ ($\Delta = \Delta\omega, \Delta t$). Entanglement is verified for outer cutoffs less than $[-4.8(\frac{\Delta}{2}), 4.8(\frac{\Delta}{2})]$.

5.5. Noise

Any actual experiment will suffer to some degree from losses, dark counts, and noise, all of which can adversely affect the ability to verify entanglement and prove security. Ref. [25] analyzes the effect of dark counts and transmission channel losses on key size, so here we will do the complementary thing and look at the effect of a generic form of noise on entanglement verification.

Since we assume that the source is located in Alice's lab, after preparing the photon pair Alice keeps one of the photons for herself and sends the other to Bob through some transmission channel. If the transmission channel is noisy the correlations between Alice and Bob's measurements will probably decrease, thus decreasing their ability to verify entanglement. Suppose the noise mechanism causes a random shift in the time of arrival of the photon

$$\tilde{f}(t_A, t_B) \rightarrow \tilde{f}(t_A, t_B + \tau_i), \tag{5.18}$$

which results in a mixed state

$$\rho = \int \mathrm{d}\tau_i P(\tau_i) |\tilde{\Psi}(t_A, t_B + \tau_i)\rangle\langle\tilde{\Psi}(t_A, t_B + \tau_i)|, \tag{5.19}$$

where

$$P(\tau_i) = \frac{1}{\sigma_\tau \sqrt{2\pi}} \exp\left(-\frac{\tau_i^2}{2\sigma_\tau^2}\right) \tag{5.20}$$

is the probability density function of τ_i, with $\int \mathrm{d}\tau_i P(\tau_i) = 1$.

This noise causes a gaussian broadening of Bob's time measurement, as seen in Figure 5.4.a This has two effects relevant to Alice and Bob's ability to verify entanglement. The first, and most significant, is that it causes a broadening in $T_-^{\delta t}$ (as seen in Figure 5.4.b), thereby increasing the Renyi entropy of $T_-^{\delta t}$ which makes it harder to verify entanglement using Eq. 5.13(or with any other criterion mentioned in the preceding chapter). The broadening also has the effect of decreasing the probability Bob will detect a photon when measuring in the time basis since more of the probability distribution is falling outside his detection range. Since the measurement results used to calculate $T_-^{\delta t}$ are conditioned on both Alice and Bob detecting photons, this means more counts must be distributed in the worst possible way, also making it harder to detect entanglement. For our parameters the latter effect leads to a relatively small change. For example, if $\sigma_\tau = 1.5\sigma_-$, the probability of both Alice and Bob detecting photons when measuring time drops from 81.3% to 80.9%. Figure 5.5. shows the minimized entanglement criterion as a function of σ_τ/σ_-. If the noise is too large (in this case $\sigma_\tau \gtrsim 1.17\sigma_-$), Alice and Bob will not be able to verify the entanglement of their shared state.

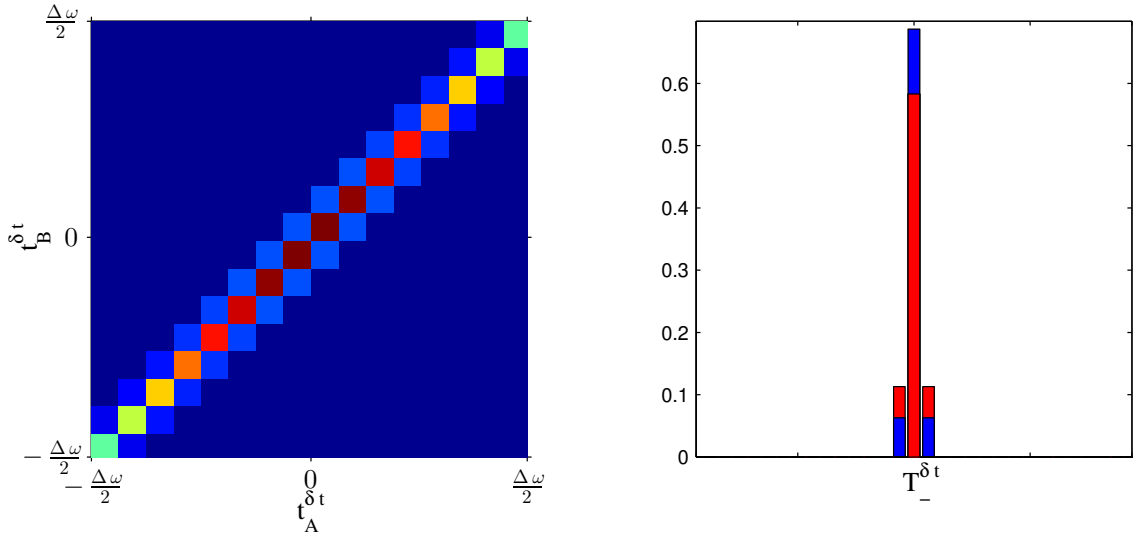

FIGURE 5.4. Left: Measured joint probability distribution for the state with time of arrival noise with $\sigma_\tau = 1.5\sigma_-$ Right: $T_-^{\delta t}$. Blue represents the original state with no noise, described by Eq. 5.16. Red is the state with time of arrival noise with $\sigma_\tau = 1.5\sigma_-$. While it may not appear that noisy, the red state will fail to be verified by the criteria.

We can also consider an additional source of noise that affects Bob's frequency measurements. We will assume that this noise affects the state in a way analogous to the time noise, namely by shifting the frequency of Bob's photon by a random amount w_j

$$f(\omega_A, \omega_B) \rightarrow f(\omega_A, \omega_B + \mathrm{w}_j), \tag{5.21}$$

which again results in a mixed state

$$\rho = \int \mathrm{dw}_j P(\mathrm{w}_j) |\Psi(\omega_A, \omega_B + \mathrm{w}_j)\rangle\langle\Psi(\omega_A, \omega_B + \mathrm{w}_j)|, \tag{5.22}$$

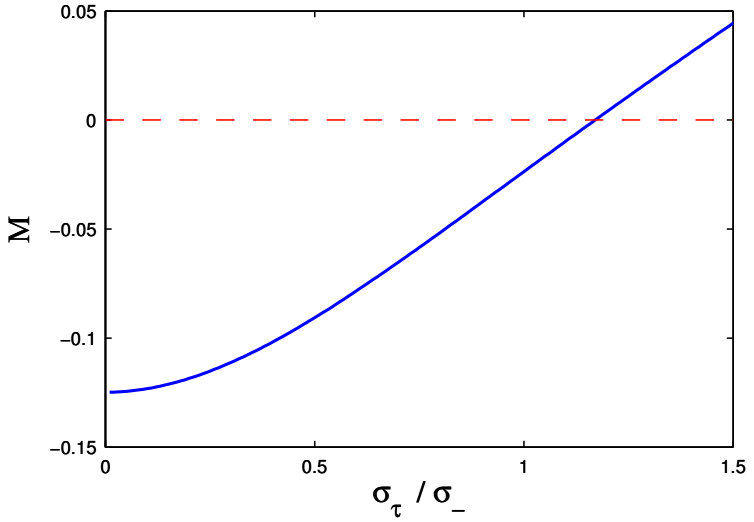

FIGURE 5.5. Optimized entanglement criteria M as a function of σ_τ/σ_- for states with time of arrival noise. Entanglement is verified when $\sigma_\tau/\sigma_- \lesssim 1.17$.

where

$$P(\mathrm{w}_j) = \frac{1}{\Lambda_\mathrm{w}\sqrt{2\pi}} \exp\left(-\frac{\mathrm{w}_j^2}{2\Lambda_\mathrm{w}^2}\right) \tag{5.23}$$

is the probability density function of w_j.

Figure 5.6. shows a contour plot of the minimized entanglement criteria M for their state with noise affecting both the time and frequency of Bob's photon. Entanglement will be verified when the combined noise is sufficiently small, as indicated by the colored region of the figure.

The state engineered and measured with the parameters chosen in [25] cannot suffer much noise before entanglement will not be verified. We expect the noise of transmission to be very small, as this is one of the advantages of using time-frequency entangled states over, for example, states carrying information in polarization or phase. Indeed, one would want to engineer the state to be sufficiently strongly correlated and the noise small enough that $\Omega_+^{\delta\omega}$ and $T_-^{\delta t}$ are confined to mostly one bin or else the quantum bit error rate will be large.

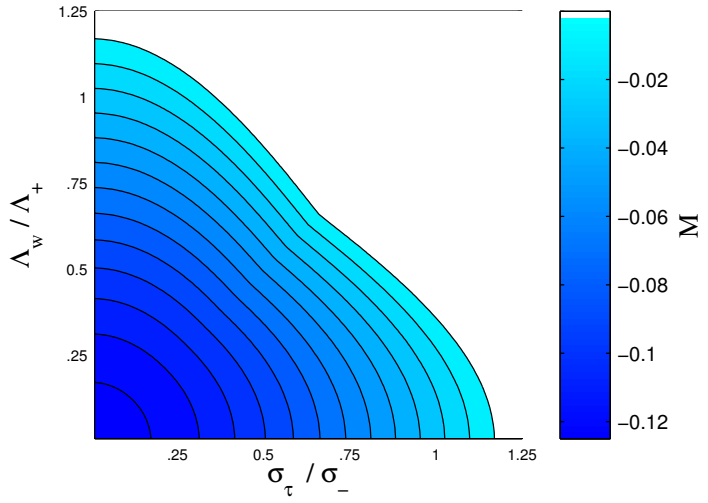

FIGURE 5.6. Optimized criterion M for states with both time and frequency noise. Entanglement is verified for colored area ($M < 0$).

That said, there are two straightforward ways to increase the amount of noise that can be tolerated while still being able to verify entanglement. The first would be to broaden the detection range to decrease the amount of missing data to a more reasonable amount, although this comes at the expense of the uniformity of the detection probability across detector bins. The other would be to increase the strength of the correlation of the state (before noise) to decrease the entropy of the data that is not missing. As technology improves a third option would be possible: to increase the resolution of the measurement to decrease the $\ln(\frac{2\pi}{\delta\omega\delta t})$ term in Eq. (5.13) for M

5.6. Conclusions

We have shown that in the absence of noise, the high-dimensional time-frequency entanglement of photon pairs for the system proposed in Ref. [25] will be verified,

even though a nonnegligible amount of data will fall outside the ranges of the time and frequency detectors. The method developed in our previous chapter for treating that type of missing data is sufficient for that purpose. We also showed that the system, due to the large amount of missing data, tolerates only low levels of noise before entanglement will no longer be verified. To increase the noise tolerance, we suggest either increasing the detection range or increasing the strength of the time- and frequency correlations.

CHAPTER VI

CONCLUSIONS

Motivated by the significance of entanglement for quantum computing and quantum cryptography, in this dissertation we looked at how to verify the presence of entanglement for two types of optical states useful for quantum information processing. We discuss these two types in order:

First, quantum computation schemes implemented with linear optics rely on the interference effects of single photons on beam splitters. One such interference effect is Hong-Ou-Mandel (HOM) interference, which results in an entangled delocalized bi-photon state: $(|02\rangle - |20\rangle)/\sqrt{2}$. In Chapter III we addressed the previously unexamined problem of verifying entanglement for states similar to the HOM state, while taking into account vacuum and multi-photon contaminations, phase noise, and other imperfections. This problem turns out to be much more difficult than verifying entanglement for the similar delocalized *single* photon state $(|01\rangle - |10\rangle)/\sqrt{2}$ [38] that results from a single photon incident on a 50/50 beam splitter. This difficulty is due to the possible multimode character of the two photon state. The method we developed uses just linear optics and photodetectors, and for single-mode photodetectors we found a lower bound on the amount of entanglement. We also discussed the difficulty of verifying entanglement when both the photodetectors and the photons have multimode character, and derived an entanglement criterion that does not require that the photons or photodetectors be single-mode. This criterion works well when the deviation from the single-mode ideal HOM state is small.

Second, continuous variable entangled states are advantageous for use in quantum key distribution schemes as they offer the ability to encode many bits per photon

(rather than just one, when using polarization). In Chapter IV we identified an important problem in continuous variable entanglement verification that surprisingly had not been addressed before: detectors used to measure continuous variables are necessarily of finite range and this may result in missing data outside the detector range. We illustrated the importance of the missing data by showing how ignoring it can lead one to falsely conclude the presence of entanglement. In the case of quantum cryptography it would lead one to falsely believe to have security. We presented a straightforward solution to this problem based on a worst-case analysis (where missing data is distributed in the most disadvantageous way possible). We described how to account for the missing data when applying either variance based or entropic entanglement criteria, and demonstrated the superiority of entropic criteria in this respect. We then applied these methods in Chapter V to a quantum key distribution scheme recently proposed by Nunn, et al. [25] which uses time-frequency entangled photon pairs. We demonstrated that our method is indeed able to verify the entanglement of the proposed state, but that noise can quickly destroy that ability as a result of the large amount of missing data.

REFERENCES CITED

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[2] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 10 1935. ISSN 1469-8064.

[3] J. S. Bell. *Speakable and Unspeakable in Quantum Mechanics: Collected papers on quantum philosophy*. Cambridge University Press, 2004.

[4] J. S. Bell et al. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[5] H. M. Wiseman, S. J. Jones, and A. Doherty. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Physical Review Letters*, 98(14): 140402, 2007.

[6] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. Pryde. Experimental epr-steering using bell-local states. *Nature Physics*, 6(11):845–849, 2010.

[7] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. Reid. Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox. *Physical Review A*, 80(3):032112, 2009.

[8] S. Aaronson. *Quantum computing since Democritus*. Cambridge University Press, 2013.

[9] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[10] S. Singh. *The code book: the science of secrecy from ancient Egypt to quantum cryptography*. Random House Digital, Inc., 2011.

[11] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, STOC '03, pages 10–19. ACM, 2003. ISBN 1-58113-674-9.

[12] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.

[13] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[14] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters*, 84(20):4729, 2000.

[15] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson. Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities. *Nature Physics*, 7(9):677–680, 2011.

[16] T. Inagaki, N. Matsuda, O. Tadanaga, Y. Nishida, M. Asobe, and H. Takesue. Long distance distribution of entangled photon pair over 300 km of fiber. In *CLEO: QELS_Fundamental Science*. Optical Society of America, 2013.

[17] R. Fickler, R. Lapkiewicz, W. N. Plick, M. Krenn, C. Schaeff, S. Ramelow, and A. Zeilinger. Quantum entanglement of high angular momenta. *Science*, 338 (6107):640–643, 2012.

[18] S. Walborn, P. S. Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner. Experimental determination of entanglement with a single measurement. *Nature*, 440(7087):1022–1024, 2006.

[19] S. J. van Enk, N. Lütkenhaus, and H. J. Kimble. Experimental procedures for entanglement verification. *Physical Review A*, 75(5):052318, 2007.

[20] C. Hong, Z. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18): 2044–2046, 1987.

[21] M. Raymer, S. J. van Enk, C. McKinstrie, and H. McGuinness. Interference of two photons of different color. *Optics Communications*, 283(5):747–752, 2010.

[22] J. L. O'Brien. Optical quantum computing. *Science*, 318(5856):1567–1570, 2007.

[23] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[24] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[25] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Optics Express*, 21(13):15959–15973, 2013.

[26] S. J. van Enk. Entanglement of electromagnetic fields. *Physical Review A*, 67(2): 022303, 2003.

[27] A. Peres. Separability criterion for density matrices. *Physical Review Letters*, 77 (8):1413, 1996.

[28] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996.

[29] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus. Detecting two-party quantum correlations in quantum-key-distribution protocols. *Physical Review A*, 71(2):022306, 2005.

[30] R. Blume-Kohout, J. O. S. Yin, and S. J. van Enk. Entanglement verification with finite data. *Phys. Rev. Lett.*, 105(17):170501, 2010.

[31] J. C. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien. Manipulation of multiphoton entanglement in waveguide quantum circuits. *Nature Photonics*, 3 (6):346–350, 2009.

[32] C. F. Wildfeuer, A. P. Lund, and J. P. Dowling. Strong violations of bell-type inequalities for path-entangled number states. *Physical Review A*, 76(5): 052101, 2007.

[33] S. B. Papp, K. S. Choi, H. Deng, P. Lougovski, S. J. van Enk, and H. Kimble. Characterization of multipartite entanglement for one photon shared among four optical modes. *Science*, 324(5928):764–768, 2009.

[34] P. Lougovski, S. J. van Enk, K. S. Choi, S. B. Papp, H. Deng, and H. Kimble. Verifying multipartite mode entanglement of w states. *New Journal of Physics*, 11(6):063029, 2009.

[35] G. Burkard and D. Loss. Lower bound for electron spin entanglement from beam splitter current correlations. *Physical Review Letters*, 91(8):087903, 2003.

[36] V. Giovannetti, D. Frustaglia, F. Taddei, and R. Fazio. Electronic Hong-Ou-Mandel interferometer for multimode entanglement detection. *Physical Review B*, 74(11):115315, 2006.

[37] V. Giovannetti. Entanglement and statistics in Hong-Ou-Mandel interferometry. *Laser Physics*, 16(10):1406–1410, 2006.

[38] J. O. Yin and S. J. van Enk. Entanglement and purity of one-and two-photon states. *Physical Review A*, 77(6):062333, 2008.

[39] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474(1):1–75, 2009.

[40] T. Zhong, F. N. Wong, A. Restelli, and J. C. Bienfang. Efficient single-spatial-mode periodically-poled ktiopo_4 waveguide source for high-dimensional entanglement-based quantum key distribution. *arXiv:1211.4496*, 2012.

[41] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *arXiv:1210.6216*, 2012.

[42] M. Yukawa, K. Miyata, T. Mizuta, H. Yonezawa, P. Marek, R. Filip, and A. Furusawa. Generating superposition of up-to three photons for continuous variable quantum information processing. *arXiv:1212.3396*, 2012.

[43] L. K. Shalm, D. R. Hamel, Z. Yan, C. Simon, K. J. Resch, and T. Jennewein. Three-photon energy-time entanglement. *Nature Physics*, 9(1):19, 2013.

[44] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nature Communications*, 3:1083, 2012.

[45] L. Zhang, C. Silberhorn, and I. A. Walmsley. Secure quantum key distribution using continuous variables of single photons. *Physical Review Letters*, 100(11): 110504, 2008.

[46] E. Shchukin and W. Vogel. Inseparability criteria for continuous bipartite quantum states. *Physical Review Letters*, 95(23):230502, 2005.

[47] A. Miranowicz, M. Piani, P. Horodecki, and R. Horodecki. Inseparability criteria based on matrices of moments. *Physical Review A*, 80(5):052303, 2009.

[48] L.-M. Duan, G. Giedke, J. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84:2722–2725, 2000.

[49] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726, 2000.

[50] M. G. Raymer, A. Funk, B. Sanders, and H. De Guise. Separability criterion for separate quantum systems. *Physical Review A*, 67(5):052104, 2003.

[51] S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi. Entangling macroscopic oscillators exploiting radiation pressure. *Physical Review Letters*, 88(12): 120401, 2002.

[52] D. Tasca, Ł. Rudnicki, R. Gomes, F. Toscano, and S. Walborn. Reliable entanglement detection under coarse-grained measurements. *Physical Review Letters*, 110(21):210502, 2013.

[53] B.-G. Englert and K. Wódkiewicz. Tutorial notes on one-party and two-party gaussian states. *International Journal of Quantum Information*, 1(02):153–188, 2003.

[54] S. Walborn, B. Taketani, A. Salles, F. Toscano, and R. de Matos Filho. Entropic entanglement criteria for continuous variables. *Physical Review Letters*, 103 (16):160505, 2009.

[55] A. Saboia, F. Toscano, and S. Walborn. Family of continuous-variable entanglement criteria using general entropy functions. *Physical Review A*, 83 (3):032307, 2011.

[56] M. Tomamichel. A framework for non-asymptotic quantum information theory. *arXiv:1203.2142*, 2012.

[57] I. Bialynicki-Birula. Formulation of the uncertainty relations in terms of the rényi entropies. *Physical Review A*, 74(5):052101, 2006.

[58] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical Review Letters*, 109(10):100502, 2012.

[59] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11):110506, 2011.

[60] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui. A new quantum key distribution scheme based on frequency and time coding. *Chinese Physics Letters*, 27(9):090301, 2010.

[61] B. Qi. Quantum key distribution based on frequency-time coding: security and feasibility. *arXiv:1101.5995*, 2011.

[62] J. Mower, F. Wong, J. H. Shapiro, and D. Englund. Dense wavelength division multiplexed quantum key distribution using entangled photons. *arXiv:1110.4867*, 2011.

[63] B. Qi. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Optics letters*, 31(18):2795–2797, 2006.

[64] O. Cohen, J. S. Lundeen, B. J. Smith, G. Puentes, P. J. Mosley, and I. A. Walmsley. Tailored photon-pair generation in optical fibers. *Physical Review Letters*, 102(12):123603, 2009.

[65] K. Garay-Palmett, H. McGuinness, O. Cohen, J. Lundeen, R. Rangel-Rojo, A. U'Ren, M. Raymer, C. McKinstrie, S. Radic, and I. Walmsley. Photon pair-state preparation with tailored spectral properties by spontaneous four-wave mixing in photonic-crystal fiber. *Optics Express*, 15:14870, 2007.

[66] O. Kuzucu, M. Fiorentino, M. A. Albota, F. N. Wong, and F. X. Kärtner. Two-photon coincident-frequency entanglement via extended phase matching. *Physical Review Letters*, 94(8):083601, 2005.

[67] W. Grice and I. Walmsley. Spectral information and distinguishability in type-ii down-conversion with a broadband pump. *Physical Review A*, 56(2):1627, 1997.

[68] G. P. Agrawal. *Nonlinear fiber optics*. Springer, 2000.

[69] I. Ali-Khan, C. J. Broadbent, and J. C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Physical Review Letters*, 98:060503, Feb 2007.

[70] M. Beck, M. Raymer, I. Walmsley, and V. Wong. Chronocyclic tomography for measuring the amplitude and phase structure of optical pulses. *Optics Letters*, 18(23):2041–2043, 1993.

[71] M. Kauffman, W. Banyai, A. Godil, and D. Bloom. Time-to-frequency converter for measuring picosecond optical pulses. *Applied Physics Letters*, 64(3): 270–272, 1994.

[72] V. Wong and I. A. Walmsley. Analysis of ultrashort pulse-shape measurement using linear interferometers. *Optics Letters*, 19(4):287–289, 1994.

[73] V. Wong and I. A. Walmsley. Linear filter analysis of methods for ultrashort-pulse-shape measurements. *JOSA B*, 12(8):1491–1499, 1995.

[74] W. Wasilewski, A. Lvovsky, K. Banaszek, and C. Radzewicz. Pulsed squeezed light: simultaneous squeezing of multiple modes. *Physical Review A*, 73(6): 063819, 2006.