Chapter 16
Quantum Information

16.1 Introduction

Quantum information theory is the study of communication and information processing tasks using physical systems that obey the rules of quantum theory. Information theory was largely the creation of Claude Shannon working at Bell laboratories over 50 years ago. Shannon produced an elegant mathematical theory for information encoding, transmission and decoding in the presence of noise. The work was grounded in a deep intuitive knowledge of the nature of noise in classical electronics and electromagnetism although it made little reference to the physical carrier of the information or the physical source of the noise. In the early 1980s a number of pioneers, including Feynman, Fredkin, Bennett, Landauer and Deutsch, began to re-consider these issues in the light of quantum noise. We now know that quantum mechanics provides powerful new ways to communicate and process information that are impossible, or difficult, in a classical world. Many of these new ideas have had an impact on quantum optics and some of the first experiments in this burgeoning field involve quantum optical systems. In this chapter we will consider some of these developments including quantum cryptography, quantum teleportation and quantum computation.

In classical information theory, the elementary unit of communication and information processing is the binary digit, or bit, which can take the mutually exclusive values 0 or 1. All communication and information processing can be reduced to operations on strings of binary digits. In 1946 Shannon [1] established a number of theorems for such operations and founded the subject of information theory [2]. Somewhat paradoxically, the key for this development lay in asking how much information is gained when the result of a random binary choice is known. Consider, for example, a fair coin toss. If we code a head as 1 and a tail as 0, it is clear that to record the result of a single coin toss we require one binary digit. When the result is known we have gained one bit of information. If we toss N coins there are 2^N possible outcomes, yet to record a single outcome requires only N bits. It would appear from this that an intuitive definition for a numerical measure of information

is the logarithm of the number of possible alternative ways a given outcome can be realised. If all outcomes are equally likely, as in the case of a fair coin toss of N coins, the probability of each outcome is 2^{-N}. The information content of a the ith outcome is then $H = -\log_2 p_i$ where $p_i = 2^{-N}$ is the probability of the outcome. The dependence of the information measure on the logarithm of the probability ensures that information is additive as our intuition with coin tosses would suggest. In general all outcomes are not equally likely. In that case we are led to define the average information of an outcome as $H = -\sum_i p_i \log_2 p_i$. We choose to define our logarithms base two as this leads to a measure of information in bits, which appears more natural in this context.

16.1.1 The Qubit

Quantum mechanics indicates that, at its most fundamental level, the physical world is irreducibly random. Given complete knowledge of the state of a physical system (that is a pure state) there is at least one measurement the results of which are completely random. The simplest example is provided by a two-state system such as a spin-half particle, a polarised photon, or a two-level atom. An elementary optical two-state system is a beam splitter, shown in Fig. 16.1. A single photon directed towards a 50/50 beam splitter will be reflected or transmitted with equal probability (we assume an ideal device that does not absorb the photon). If we place a perfect photon detector in both output ports of the beam splitter we will get a count at one or the other detector with equal probability. At first sight it would appear that a single two-state system such as this is a perfect quantum coin toss, but the reality is more subtle.

To understand why this is so consider the example depicted in Fig. 16.2 in which we try to toss the quantum coin twice in succession by redirecting the photon towards another identical beam splitter. In a real coin toss the outcome is no less

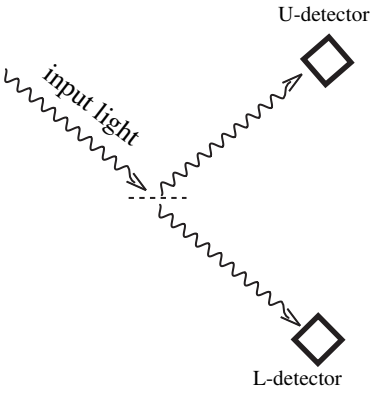

Fig. 16.1 A single photon at a 50/50 beam splitter can be reflected or transmitted with equal probability. A perfect photon detector in both output ports of the beam splitter, labeled U (*upper*) or L (*lower*), will register a count at one or the other detector with equal probability

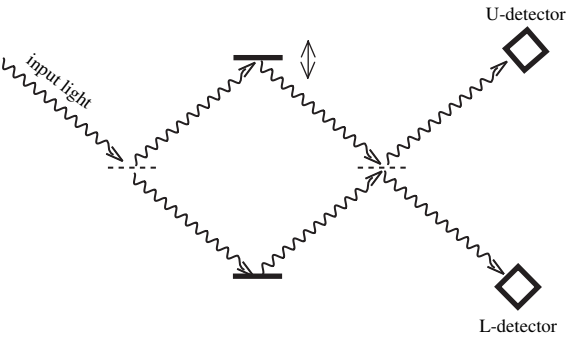

Fig. 16.2 Tossing a quantum coin twice. After the first beam splitter in Fig. 16.1, a single photon is redirected, using perfectly reflecting mirrors, towards an identical beam splitter. The device is now a Mach–Zehnder interferometer and can be adjusted, by moving a mirror as indicated, so that the photon emerges with certainty in the upper output mode. The adjustment can be made by small displacements on one of the perfectly reflecting mirrors

uncertain than the first coin toss. Such is not the case for this "quantum coin toss". In Fig. 16.2 we illustrate a possible way to make the photon choose twice in succession whether to be reflected or transmitted, and immediately recognise the form of a Mach–Zehnder interferometer. Clearly we can set up this device so that the photon will be detected with certainty in say the upper photon detector. This is very different from tossing two coins in succession.

The explanation of this phenomenon takes us to the heart of why quantum information theory will necessarily be different from classical information theory. Immediately after the first beam splitter the photon is in a quantum superposition of two distinct spatial modes of the field;

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_U \otimes |0\rangle_L + |0\rangle_U \otimes |1\rangle_L) \tag{16.1}$$

where we have labelled the two output modes as up (U) or lower (L). If we place a photon detector in both output modes it is easy to see that we will count a photon in each mode with equal probability. However the state is not a truly random state. In fact it is a pure state, the entropy of which is zero. The beam-splitter has unitarily transformed the initial pure state $|0\rangle_U \otimes |1\rangle_L$. If the system is caused to pass through another beam splitter a further unitary transformation takes place which, for appropriate path lengths, will produce the state $|1\rangle_U \otimes |0\rangle_L$ at the output and the photon will be detected with certainty in the upper detector.

We need to distinguish a true coin toss from a "quantum" coin toss. The key distinguishing feature is the ability of the quantum system to be prepared in a coherent superposition of the two mutually exclusive alternatives. This is not possible for a classical coin toss which is either heads or tails but not both. While it is true that the result of an arbitrary measurement on a single two state system will give one bit of information in general, the system state is not like a classical coin toss, as the single photon example illustrates. To distinguish a true one bit classical system from a quantum one bit system we will refer to the quantum case as a *qubit*. A qubit is then

a quantum system which can yield at most one bit of information upon measurement, but which can be in a coherent quantum superposition of the two mutually exclusive outcomes prior to measurement. In the case of N qubits the system can exist in a superposition of all 2^N possible product states of each individual qubit. It is this exponential rise in the number of states accessible to an N qubit system that gives quantum information processing its power. We discuss below an example of how even a single qubit can be harnessed to do things that a classical one bit system never could; secure key distribution.

16.1.2 Entanglement

The key feature of quantum mechanics that lies behind quantum information theory is quantum entanglement. Quantum entanglement refers to correlations between the results of measurements made on distinct subsystems of a composite system that cannot be explained in terms of standard statistical correlations between classical properties inherent in each subsystem. An example is provided by the violation of the Bell inequality for two distinct two-state quantum systems (see Chap. 13). If the subsystems are time like separated, quantum entanglement implies non-locality. Non-locality means that measurements on distinct subsystems, local measurements, are incapable of determining the joint state of the composite system. While quantum entanglement and non-locality are related they are not the same. It is possible to have non-locality without entanglement [3].

In quantum optics the simplest source of entanglement is provided by the non-degenerate squeezed vacuum state produced by spontaneous parametric down conversion (see Sect. 5.2.1),

$$|\mathscr{E}\rangle = (1-\lambda^2)^{1/2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_a \otimes |n\rangle_b \tag{16.2}$$

where $\lambda = \tanh r$ with r the squeezing parameter. Note that this state is a zero eigenstate of the photon number difference operator, $\hat{n}_a - \hat{n}_b$, between the two modes. The entanglement here results from a superposition of the infinite number of indistinguishable ways we can distribute equal numbers of photons in each mode. The reduced state of each subsystem (modes a and b) is in fact a thermal state (see Sect. 5.2.5). This is the maximum entropy state for a mode with a fixed average energy. Thus while the total state is a pure state with zero entropy, the state of each subsystem is as uncertain as it can be given the constraint on the average energy.

Measurements on the component sub-systems of entangled states are insufficient to completely determine the joint state of the system. In some cases local measurements may give no information at all about the joint state and the entropy of the subsystem reduced states are maximal. Such states are called maximally entangled.

An example is provided by the following eigenstates of total photon number,

$$|\psi_N\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} |n\rangle_a \otimes |N-n\rangle_b \tag{16.3}$$

Local measurements on either mode, say a, are described by the reduced density operator

$$\rho_a = \mathrm{Tr}_b(\rho) \tag{16.4}$$

where Tr_b refers to the partial trace over mode b. In this case the resulting reduced density operator for each mode is the identity matrix in $N+1$ dimensions. The entropy of such a state is

$$S_{a,b} = -\mathrm{Tr}\rho_{a,b} \ln \rho_{a,b} = \ln(N+1) \tag{16.5}$$

which, given the constraint on total photon number, is maximal. In general the entropy of each subsystem satisfy an important inequality, the Araki–Lieb inequality,

$$|S_a - S_b| \leq S \leq S_a + S_b \tag{16.6}$$

where S is the entropy of the state of the joint system. In the case of a pure entangled state this implies that $S_a = S_b$.

Entangled states do not necessarily need to be pure states. Furthermore there can be non-entangled states that still exhibit classical correlations between the subsystems. If an entangled state interacts with an environment entanglement can be reduced to zero while classical correlations remain. An example is provided by a two-mode squeezed vacuum state undergoing phase diffusion in each mode. The steady state density operator describing such a system is

$$\rho = (1-\lambda^2) \sum_{n=0}^{\infty} \lambda^{2n} |n\rangle_a\langle n| \otimes |n\rangle_b\langle n| \tag{16.7}$$

which still retains a perfect classical correlation between the photon numbers in each mode. However as the state is a convex sum of states which factorise, the state in (16.7) is not entangled and in fact is defined as separable.

It seems reasonable to suggest that between pure entangled states and totally separable mixed states there is a gradation of entanglement. To quantify this we require a measure of entanglement, and a number of such measures for finite dimensional Hilbert spaces have been proposed [4]. The situation for infinite dimensional Hilbert spaces, which is the case for much of quantum optics, is complicated except for a special class of states known as Gaussian states. Such states have a Gaussian Wigner function. The two mode squeezed state is an example (see Sect. 5.2.4). Further discussion on mixed Gaussian entangled states is given in [5]

When a pure state, $|\psi\rangle$ interacts with an environment it undergoes decoherence (see Chap. 15) and generally becomes a mixed state, ρ. We can then ask for the probability of finding the initial state, ψ in the ensemble represented by ρ.

This probability is given by

$$F = \mathrm{Tr}(\rho|\psi\rangle\langle\psi|) \tag{16.8}$$

which is called the fidelity. Fidelity has a deeper significance in terms of the statistical distinguishability of quantum states [6].

16.2 Quantum Key Distribution

For millennia, communicating parties have devised schemes whereby messages can be authenticated (the signature) and secured from unauthorised access (cryptography). Modern methods (symmetrical crypto-systems) for secure electronic communication involve the prior exchange of a random number which is called the key. If the communicating parties share this number with each other and no one else, messages can be securely encrypted and decoded. The method however is vulnerable to a third party acquiring access to the key. In this section we will describe how quantum mechanics enables two communicating parties to arrive at a shared secure key via Quantum Key Distribution (QKD).

The idea that quantum mechanics might enable more secure communication was hinted at in the work of Wiesner [7] and made explicit in the pioneering work of Bennett and Brassard [8], in which the first QKD protocol, BB84, was presented. It uses a set of four qubit states to encode one bit. The first experimental demonstration of QKD was made by Bennett, Brassard and co-workers in 1989 [9]. The first practical implementation over a kilometer of optical fibre was achieved by Gisin's group in Geneva [10]. The idea has since been elaborated by a number of authors including Ekert [11] who in 1991 showed that EPR entangled states of pairs of photons could also be used for QKD. However here we will describe the minimal QKD scheme of Bennettt, B92 [12], as this scheme is simpler than BB84 (it uses only two non orthogonal states) and has been successfully implemented in optical fibres over long distances and in free space communication. In practice however a two state QKD scheme is not desirable as it is possible to distinguish two non orthogonal states provided we accept inconclusive outcomes in some trials.

The key idea behind QKD is the Heisenberg uncertainty principle which ensures that any attempt to measure a quantum state will change it, and thus eavesdropping can in principle be detected. This is related to a powerful theorem in quantum information theory, the "no-cloning" theorem: an unknown quantum state cannot be duplicated [13]. Thus experimental QKD offers important new insights into the nature of quantum physics. Let us now follow a classical protocol to establish a shared random key between two communicating parties, called Alice (A) and Bob (B).

Alice and Bob are assumed to have a means to generate completely random binary numbers. Alice generates a random binary number and sends it to Bob, and Bob generates a random binary number and compares it to the binary number received from Alice. If it is the same he tells Alice publicly that this is the case, but does *not* reveal what the value actually was. If it was the same, Alice and Bob

keep this binary number, otherwise they discard it. Alice and Bob then repeat the procedure for another binary number and continue in this way until they share a binary string that is a subset of the total binary string that Alice sent to Bob. If for some reason Alice's binary number fails to get to Bob in a particular run, it makes no difference to the final shared binary string (although it does reduce the rate of communication for the shared binary string). The big problem with this method is that classically it is possible for an eavesdropper, Eve, to copy Alice's transmitted binary number without disturbing it. Then Eve can listen to the public channel and hear Bob telling Alice that this number was the same as his binary number. QKD avoids this problem by making it impossible for Eve to measure (or copy) an unknown quantum state without also disturbing it in general. If Alice and Bob chose carefully the quantum state encoding their binary numbers an eavesdropper can be detected by Alice and Bob.

Alice and Bob will communicate with polarised single photon pulses (see Sect. 16.4.2 for further discussion). They first need to agree on how to physically implement the encoding. Suppose Alice decides to transmit only vertically (V) and $+45^{\mathrm{o}}$ $(+D)$ photons. She will send a V-photon when a previously generated random binary number is a 0 and a +D-photon when the random binary number is a 1.

$$A: \quad V \leftrightarrow 0; \quad +D \leftrightarrow 1\,. \tag{16.9}$$

Bob and Alice also agree that Bob can make a polarisation *measurements* of Alice's photon in only two directions; horizontally (H) or at -45^{o} $(-D)$. These measurements project onto non-orthogonal polarisation states. Bob randomly decides which of his two allowed measurements he will make on any photon he receives from Alice. The choice of measurement is made by referring to a previously generated random bit according to the code,

$$B: \quad 0 \leftrightarrow -D; \quad 1 \leftrightarrow H\,. \tag{16.10}$$

When Bob measures the polarisation he records the result as a yes (Y) or a no (N) depending on whether the photon was indeed found to have that particular polarisation. Bob will never record a Y if his bit is different from Alice's (crossed polarisers), and he records a Y on 50% of runs in which their bits are the same. Thus Bob can only get a Y if his bit is the same as Alice's (although he may get a N in that case as well). Finally Bob sends a copy of his results to Alice, over a public channel, but he does not tell Alice what measurement he made on each bit. Now Alice and Bob retain only those bits for which Bob's result was "Y". These bits are the shared key.

If Eve, an eavesdropper, makes a QND polarisation measurement of Alice's transmitted photons in an attempt to learn what was sent, she will introduce a 25% error rate between Alice and Bob's shared key. This occurs because her measurement will project the transmitted state into the eigenstates corresponding to her measurement result and this state may be different from that sent by Alice. Alice and Bob can test for eavesdropping by agreeing to sacrifice part of their shared key to check the error rate. If the error rate is 25% or higher they will suspect an

eavesdropper and discard the entire shared key. In reality errors are inevitable, and Alice and Bob will need to agree on an acceptable error threshold less than 25%.

This protocol has been demonstrated experimentally by the group of Hughes at Los Alamos National Laboratory. The requirement that we use single photon states to code the bits of information places considerable demands on the physical resources required to implement B92. A considerable effort is being expended to realise single photon pulsed sources. Given such a source we also need to be able to reliably detect single photons, with a small dark count rate, and we need to propagate single photon pulses over possibly large distances with as little loss as possible. If the loss rate is too high very few counts will be available to Alice and Bob to construct their shared key and thus the data transmission rate could be unacceptably low. Finally, if we are to use standard optical fibres to transmit the photons, polarisation encoding is difficult owing to the birefringence of optical fibres.

To overcome this last problem the Los Alamos experiment used an interferometric implementation of B92 [14]. We can use any two state system to represent a qubit and thus any two state system can in principle be used for QKD. An example is provided by a single photon Mach-Zhender (M-Z) interferometer, see Fig. 16.3. The M-Z interferometer couples two input modes to two output modes, labelled U (for upper) and L (for lower) in Fig. 16.3. The device provides two possible paths for a single photon input at say U to be transmitted to the output. If path lengths are equal we can set up the device so that a photon input at U will be counted with certainty at the L-detector. However we also have the freedom to insert phase shift devices into either path and thus change the interference conditions. In particular Alice can insert a phase shift ϕ_A into one end of the device co-located with her transmission while

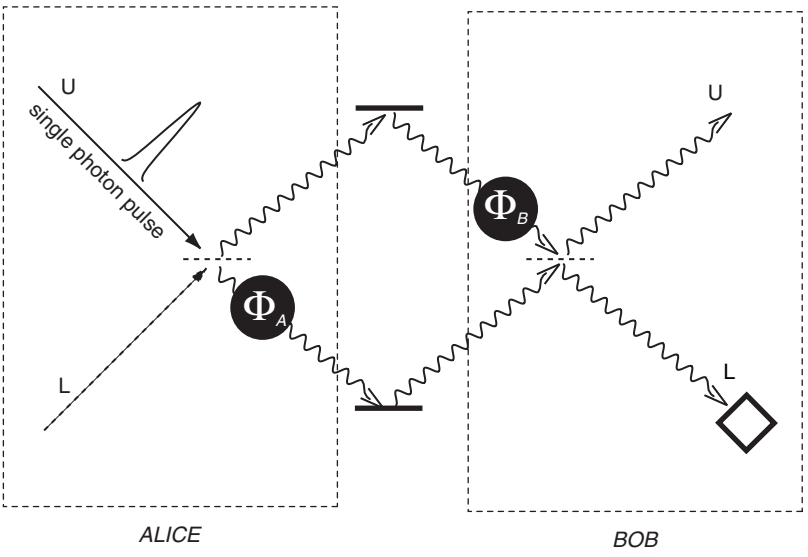

Fig. 16.3 A method to use phase shift coding for coherent pulses in a QKD protocol

Bob can insert another phase shift ϕ_B co-located with his reception. Let us assume Alice injects photons into the U input mode and that Bob counts photons only from the L detector mode. The input state is $|1\rangle_U|0\rangle_L$. The beam splitters implement the state transformations,

$$|1\rangle_U|0\rangle_L \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_U|0\rangle_L + |0\rangle_U|1\rangle_L) \tag{16.11}$$

$$|0\rangle_U|1\rangle_L \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_U|1\rangle_L - |1\rangle_U|0\rangle_L) \tag{16.12}$$

The output state is thus given by

$$|\Psi\rangle_{\text{out}} = \frac{1}{2}\left(e^{i\phi_B} - e^{i\phi_A}\right)|1\rangle_U|0\rangle_L + \frac{1}{2}\left(e^{i\phi_B} + e^{i\phi_A}\right)|0\rangle_U|1\rangle_L \tag{16.13}$$

The probability that a photon injected by Alice is detected by Bob is then

$$P_{\text{D}} = \cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \tag{16.14}$$

Now if Alice and Bob use phase angles $(\phi_A, \phi_B) = (0, 3\pi/2)$ to encode 0 and $(\phi_A, \phi_B) = (\pi/2, \pi)$ to encode 1, they have an exact realisation of B92, where polariser angels are replaced by path length differences.

To realise a M-Z interferometer using optical fibres for each of the paths is difficult if the arms extend over large distances. Small fluctuations in phase shifts along each path would lead to a very unstable interferometer. In the Los Alamos experiment this problem was overcome using a single optical fibre for both arms with a unbalanced M-Z interferometer (a Franson-type interferometer) at either end, see Fig. 16.4.

In this scheme there are two paths for a single photon at each end, a "long" path and a "short" path. Thus the four possible histories of a photon can be conveniently described as; short-short (SS), long-long (LL), short-long (SL) and long-short(LS). As the last two histories are indistinguishable we expect to see interference between these two processes. When a single photon pulse passes though Alice's M-Z interferometer the output state is a superposition of two pulses delayed by a time T

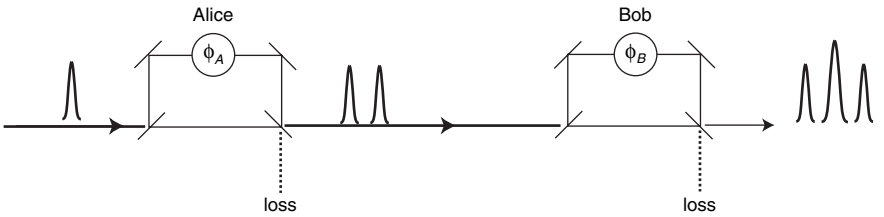

Fig. 16.4 A method to implement time multiplexed codes for QKD. From "Secure communications using quantum cryptography" [14]

equal to the delay between the short and the long path. At the output of Bob's M-Z interferometer there will be three pulses, one leading 'prompt' pulse corresponding to the history SS, one delayed pulse corresponding to LL and one central pulse corresponding to the two interfering possibilities SL and LS. Of course not every photon makes it to Bob's output port: each M-Z interferometer has two output ports and some photons exit in the "loss" ports in Fig. 16.4. As there is no interference in LL and SS the photons arrive in these time windows with a probability of $1/16$ for $50/50$ beam splitters. However the probability of detecting a photon in the central pulse is

$$P_D = \frac{1}{4}\cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \tag{16.15}$$

Note that this is the same as the previous single M-Z scheme apart from the additional factor of $1/4$. Thus we can implement the M-Z version of B92 provided we are prepared to sacrifice detection events so that the data rate is at least reduced by a factor of 4.

In the Los Alamos experiment the two unbalanced M-Z interferometers were constructed using 50/50 fibre couplers. The long arm of the device corresponded to a standard underground optical fibre link 24 km long. The total travel time over the underground link is about 80 μs, with 10 DBE of attenuation due to the fibre's 0.3-dB/km attenuation and four connections along the path. Photons emerge from one of the output legs of Bob's interferometer into a cooled InGaAs APD detector. The photons at Alice's end are generated by a 1.3 μm pulsed semiconductor laser. A 300-ps electrical pulse is applied to the laser, with a 10-kHz repetition rate. A laser of course does *not* produce pulses with one and only one photon per pulse but rather generates a coherent state with a Poisson distribution of photons per pulse. However if we attenuate the output pulse so that on average there is only a singe photon we can get a very close realisation of the B92 protocol. The possibility that a pulse contains 2 or more photons is a potential loop hole for an eavesdropper to exploit, and thus there is some motivation to consider developing a true single photon source for this implementation. Each "single-photon" pulse is preceded by a bright reference pulse, introduced to the lower input port of Alice's interferometer, to provide arrival time information to Bob. This bright pulse triggers a room-temperature detector in the upper output port of Bob's interferometer, which provides the "start" signal for a time-interval analyser. In addition to the quantum channel (24 km of optical fibre) connecting Alice and Bob there is also a public ethernet channel which allows Alice and Bob to extract a shared key.

In Fig. 16.5 we show an example of photon arrival time spectra for four different phase differences. Photon counts were accumulated for 60 s at each phase setting. The 3-ns separation of the different paths is clearly visible, as is the 300-ps width of the laser pulse. The unequal height of the "short-short" (left-most in each plot) and "long-long" (right-most) peaks is due to attenuation at the phase shifters. The average number of photons per laser pulse arriving in the central peak maximum was $n = 0.4$. After accounting for background noise an underlying interferometric visibility of $98.4 \pm 0.6\%$ was determined for the central peak. This visibility is not as

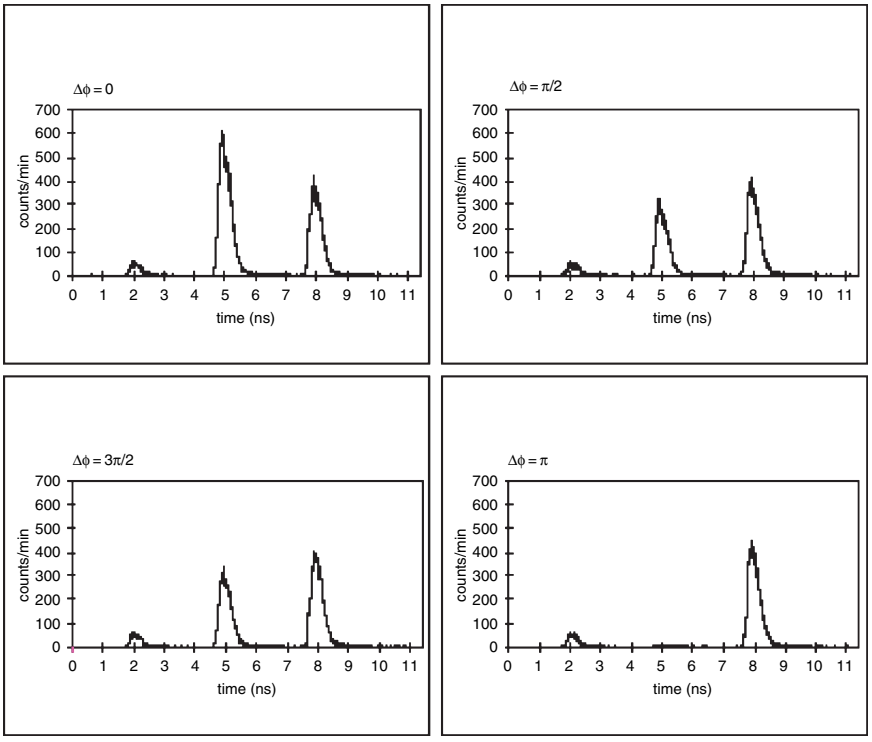

Fig. 16.5 Photon arrival time spectra for a QKD protocol discussed in the text. From "Secure communications using quantum cryptography", [14]

useful as the total probability of a count in the central time-window when the phase difference is π, because this quantity determines the error rate of the B92 protocol.

The performance of an experimental QKD system is stated in terms of the number of bits per second of a shared secret key (the distilled bit rate R_{dis}) and the distance between the communicating parties. It is usually easier to determine the raw bit rate (R_{raw}). This is determined by actual losses in the quantum channel, sources and detectors as well as possible intervention of an eavesdropper. From this the error rate in the sifted key (obtained after Alice and Bob perform a round of classical communication to reconcile their bases) is called the quantum bit error rate (QBER). The QBER for the Los Alamos experiment was 1.6%. The rate of key generation is necessarily lower than the laser pulse rate if attenuated coherent states are used instead of single photon pulses as most pulses contain no photons at all. Obviously a single photon source is desirable. We will return to this issue in Sect. 16.4.2. Furthermore there is the intrinsic inefficiency in the protocol due to a factor of 4 reduction (16.15). Along the way fibre losses and detector inefficiencies diminish the rate still further.

Quantum key distribution systems are now functioning in many laboratories around the world. A QKD system using optical fibre over 148.7 km was

demonstrated by a Los Alamos/NIST collaboration using the BB84 protocol [15]. Commercial systems are available, including id Quantique based in Geneva, MagiQ Technologies in New York and SmartQuantum in France. A number of commercial and government installations are already in place. All current systems however do not use single photon sources, but rather very weak laser pulses. These suffer from a weakness: the number of pulse in each pulse is not fixed but can fluctuate. This opens up the system to difficult but possible eavesdropper attack.

16.3 Quantum Teleportation

Quantum key distributions is the simplest quantum communication task in that it requires only the ability to coherently manipulate the state of a single qubit. Ultimately it relies on the Heisenberg uncertainty principle. Quantum teleportation is a communication task that relies on the quantum entanglement of two qubits. The objective of quantum teleportation is to take an unknown quantum state of some physical degree of freedom, which we will call the *client* (C), and using measurement and classical feed-forward control, to remotely prepare another physical degree of freedom, the *receiver*(B), in the same state, *without ever learning anything about the quantum state thus transmitted*. This is only possible if co-located with the client system there is another physical system, the *sender* (A), which is entangled with the state of the physical system at the receiver (B)(see Fig. 16.6).

Bennett et al. [16] first proposed this communication protocol in terms of systems with a two dimensional Hilbert space (qubits[17]). Inspired by a proposal of Braunstein and Kimble[18], Furasawa et al. [19] demonstrated that the method can also be applied to entangled systems with an infinite dimensional Hilbert space, specifically for harmonic oscillator states. This is known as continuous variable teleportation as it requires the ability to make measurements of observables with a continuous spectrum.

The scheme of Braunstein and Kimble was itself based on a simpler, though less practical, scheme proposed by Vaidman[20] . Vaidman showed that continuous variable teleportation is possible using the EPR entangled state (see Sect. 13.1) of two degrees of freedom. This state is the result of making a perfect quadrature phase QND (quantum nondemolition, see Chap. 14) measurement between two optical modes, A and B, to create the entanglement resource. To take this example further see Exercise 16.1. The EPR state is not a physical state because quadrature phase eigenstates are infinite energy states. However we can use arbitrary close approximations to these states in terms of a squeezed vacuum state, (16.16). This is essential feature exploited in the scheme of Furasawa et al.

Suppose that at some prior time a two mode squeezed vacuum state is generated and that one mode is available for local operations and measurements at the sender's location A by observer Alice, while the other mode is open to local operations and measurements in the receiver's location B, by observer Bob. Alice and Bob can communicate via a classical communication channel. Thus Alice and Bob each have

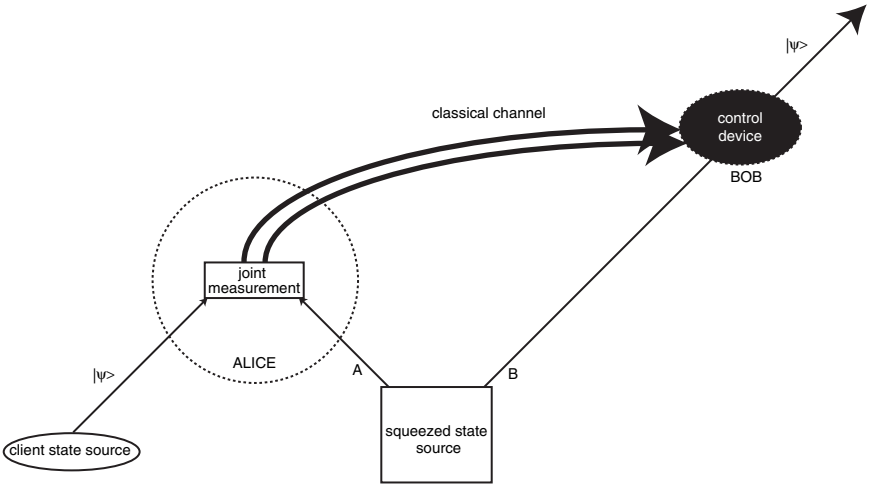

Fig. 16.6 A teleportation protocol. The sender, Alice, shares one mode A of a two-mode squeezed state, and another mode, the client, the state of which is unknown to her. Alice makes a measurement of the sum of the quadrature phase amplitudes of the client mode and mode A. The results of the measurement are sent via a classical channel to the receiver, Bob, who conditional on the information received, applies a unitary control to his share of the two-mode entangled state, mode B. The output of Bob's action is a mode now prepared in the same state as the client mode, but neither Alice or Bob learn what this state is

access to one of the two entangled subsystems described by

$$|\mathscr{E}\rangle_{AB} = \sqrt{(1-\lambda^2)}\sum_{n=0}^{\infty}\lambda^n|n\rangle_A \otimes |n\rangle_B \tag{16.16}$$

This state is generated from the vacuum state by the Unitary transformation

$$U(r) = e^{r(a^\dagger b^\dagger - ab)} \tag{16.17}$$

where $\lambda = \tanh r$ and where a, b refer to the mode accessible to Alice and the mode accessible to Bob respectively (see figure 16.6).

The entanglement of this state can be viewed in two ways. Firstly as an entanglement between quadrature phases in the two modes (EPR entanglement) and secondly as an entanglement between number and phase in the two modes (see exercise 2). We can easily show that this state approximates the entanglement of an EPR state in the limit $\lambda \to 1$ or $r \to \infty$. The quadrature phase entanglement is easily seen by calculating the effect of the squeezing transformation Eq(16.17) in the Heisenberg picture. We first define the quadrature phase operators for the two modes

$$\hat{X}_A = a + a^\dagger \tag{16.18}$$
$$\hat{Y}_A = -i(a - a^\dagger) \tag{16.19}$$
$$\hat{X}_B = b + b^\dagger \tag{16.20}$$
$$\hat{Y}_B = -i(b - b^\dagger) \tag{16.21}$$

Then

$$Var(\hat{X}_A - \hat{X}_B) = 2e^{-2r} \tag{16.22}$$
$$Var(\hat{Y}_A + \hat{Y}_B) = 2e^{-2r} \tag{16.23}$$

where $Var(A) = \langle A^2 \rangle - \langle A \rangle^2$ is the variance. Thus in the limit of $r \to \infty$ the state $|\mathscr{E}\rangle$ approaches a simultaneous eigenstates of $\hat{X}_A - \hat{X}_B$ and $\hat{Y}_A + \hat{Y}_B$. This is the analogue of the EPR state with position replaced by the real quadratures $\hat{X}$ and the momentum replaced by the imaginary quadratures, $\hat{Y}$.

Let us suppose the unknown state we wish to teleport, the client state, is written as $|\psi\rangle_C$. By this we mean that some party has prepared this mode in state $|\psi\rangle_C$, but this preparation procedure remains unknown to A and B. Perfect (projective) measurements are made of the joint quadrature phase quantities, $\hat{X}_C - \hat{X}_A$ and $\hat{Y}_C + \hat{Y}_A$ on the client mode and the Alice's part of the entangled mode, A, with the results X, Y respectively. The conditional state resulting from this joint quadrature measurement (see Exercise 16.2) is described by the projection onto the state $|X,Y\rangle_{CA}$ where

$$|X,Y\rangle_{CA} = e^{-\frac{i}{2}\hat{X}_A\hat{Y}_C}|X\rangle_C \otimes |Y\rangle_A \tag{16.24}$$

The (unnormalised) conditional state of total system after the measurement is then seen to be given by

$$|\tilde{\Psi}^{(X,Y)}\rangle_{out} = {}_{CA}\langle X,Y|\psi\rangle_C|\mathscr{E}\rangle_{AB} \otimes |X,Y\rangle_{CA} \tag{16.25}$$

The state of mode B at the receiver, denoted as Bob, is the pure state

$$|\phi^{(X,Y)}(r)\rangle_B = [P(X,Y)]^{-1/2}{}_{CA}\langle X,Y|\psi\rangle_C \otimes |\mathscr{E}\rangle_{AB} \tag{16.26}$$

with the wave function (in the $\hat{X}_B$ representation),

$$\phi_B^{(X,Y)}(x) = \int_{-\infty}^{\infty} dx' e^{-\frac{i}{2}x'Y}\mathscr{E}(x,x')\psi(X+x') \tag{16.27}$$

where $\psi(x) = {}_C\langle x|\psi\rangle_C$ is the wavefunction for the client state we seek to teleport. The kernel is simply the wave function for the two mode squeezed state resource.

The state in (16.27) is clearly not the same as the state we sought to teleport. However in the limit of infinite squeezing, $r \to \infty$, we find that $\mathscr{G}(x_1,x_2;r) \to \delta(x_1+x_2)$ and the state of mode B approaches

$$|\phi_{XY}(r)\rangle_B \to e^{-\frac{i}{2}Y\hat{X}_B}e^{\frac{i}{2}X\hat{Y}_B}|\psi\rangle_B \tag{16.28}$$

which, up to the expected unitary translations in phase-space, is the required teleported state.

For finite value of the squeeze parameter, r, the state after Bob's conditional control is not an exact replica of the client state. We can quantify how the state differs by computing the probability that the state in Bob's mode, after displacement, is the same as the state of the client mode. This probability is called the *fidelity* and is given by

$$F = |\langle\psi|e^{\frac{i}{2}\mu\hat{X}_B}e^{-\frac{i}{2}\nu\hat{Y}_B}|\phi^{(X,Y)}\rangle|^2 \tag{16.29}$$

with $\mu = gY, \nu = gX$ which allows for some flexibility in the choice of displacements in the non ideal case. The quantity g is called the *gain*. In the limit of infinite squeezing we expect $g \to 1$.

Quite apart from the limitations on the fidelity that arise from finite squeezing, other limitations arise in the real world. Noise and uncertainty can enter through imperfect measurements, though the classical communication channel, through degradation of the entanglement due to uncontrollable interactions with the environment and though imperfections in the local unitary transformations in the feed forward correction stage. These problems all limit the extent to which mean that Bob's state matches the state of the client degree of freedom. For these reasons it is necessary to validate the teleportation channel explicitly by using known client states. This will require running a number of trials with different client states and repeated measurements upon the output state at mode B. From trial to trial the state that leaves the channel at mod B will fluctuate, which means we must describe the teleported state as a mixed state, ρ_B, in general. For a fixed input client state, the probability of reproducing it at the output is given by the fidelity

$$F = \langle\psi|\rho_B|\psi\rangle \tag{16.30}$$

If we use an ensemble of client states, an overall measure of performance in terms of the average fidelity $\bar{F}$ obtained by averaging the fidelity over the ensemble of client states, $|\psi\rangle$, with some appropriate measure on the set of pure states. If the client states are drawn from an ensemble of coherent states we can obtain an explicit result. In the extreme case that A and B share no entanglement, $\bar{F} = \frac{1}{2}$., which gives a classical boundary for teleportation of a coherent state. A demonstrable quantum teleportation channel would need to give an average fidelity greater than this.

The group of Kimble at Caltech[19] were the first to demonstrate a teleportation channel using squeezed states. Similar experiments have been reported by the group of di Martini in Rome [21] and Zeilinger in Innsbruck[22]. We will take a closer look at the Caltech experiment to explain how some of the formal steps in the preceding analysis are done in the laboratory. This will also enable us to identify the sources of imperfections, such as photon loss, and noise. A schematic diagram of the experiment is given in Fig. 16.7.

In order to effect a joint measurement of the combined quadratures $\hat{X}_C - \hat{X}_A, \hat{Y}_C + \hat{Y}_A$, the experiment first combined the client and sender field amplitudes on a 50/50 beam splitter, followed by direct homodyne measurements of the output fields after the beam splitter. After the beam splitter we then make a homodyne measurement of

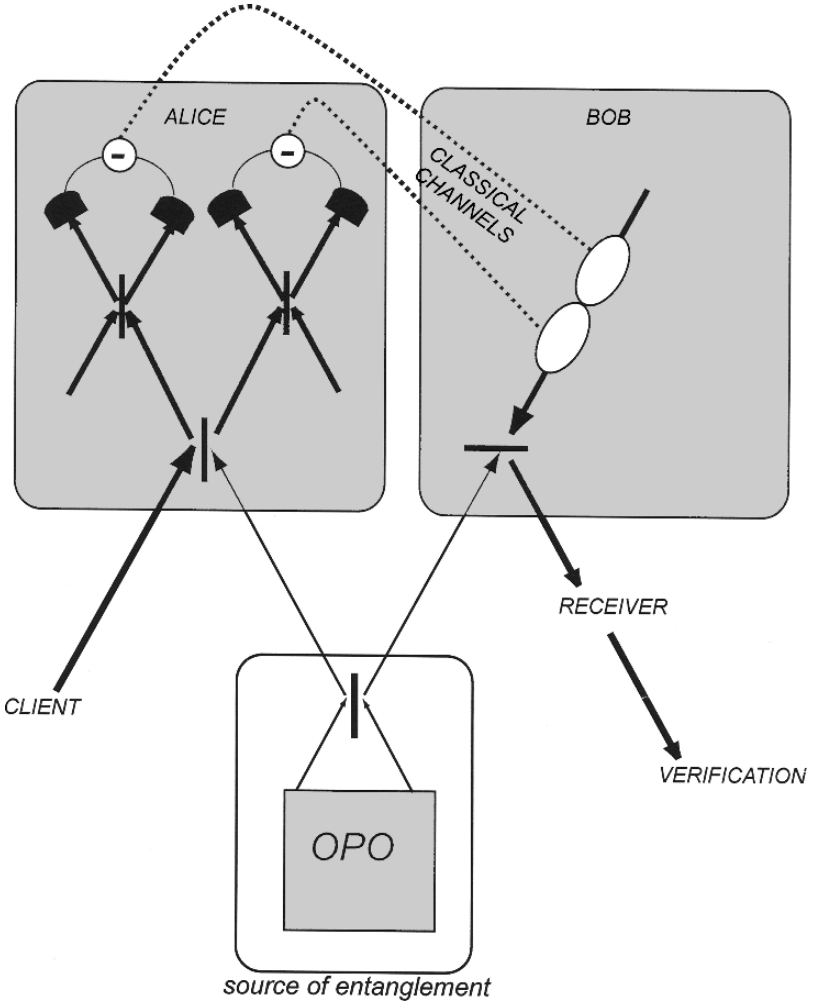

Fig. 16.7 A schematic of the Caltech teleportation experiment. An unknown quantum state is received from the client and mixed with one mode of a two mod entangled state at the sending party, Alice (A). A joint quadrature phase measurement is made by A and the results sent to a receiving party, Bob (B) though a classical channel. Given this information B then transforms the component of the shared entangled state held at B, by conditional displacements, to complete the protocol. In a checking step a state verification is undertaken by the client to determine the success of the teleportation

X-quadrature on mode C and the Y-quadrature on mode A. In the case of homodyne detection, the actual measurement records are two photo-currents (I_X, I_P). For unit efficiency detectors, this is an optimal measurement of the corresponding quadratures $\hat{X}_C, \hat{Y}_A$. In reality however efficiency is not unity and some noise is added to the measurement results. We shall return to this point below.

The measured photo-currents are a classical stochastic processes and may be sent to the receiver, B, over a standard communication channel. On receipt of this information the receiver must apply the appropriate unitary operator, a displacement, to complete the protocol. Displacement operators are quite easy to apply in quantum optics. To displace a mode, say B, we first combine it with another mode, prepared in a coherent state with large amplitude, $\alpha \rightarrow \infty$, on a beam splitter with very high reflectivity, $R \rightarrow 1$, for mode B. If $|\phi\rangle_B$ is the state of B, then after the combination at the beam splitter the state of B is transformed by

$$|\phi\rangle_B \rightarrow D(\beta)|\phi\rangle_B \tag{16.31}$$

where $D(\beta) = \exp(\beta b^\dagger - \beta^* b)$ is the unitary displacement operator, and

$$\beta = \lim_{R\rightarrow 1} \lim_{\alpha\rightarrow\infty} \alpha\sqrt{1-R} \tag{16.32}$$

In terms of the quadrature operators for B the displacement operator can be written

$$D(x,y) = e^{iy\hat{X}_B + ix\hat{Y}_B} \tag{16.33}$$

with $\beta = x + iy$. A suitable choice of β will produce the required displacements to complete the teleportation protocol. This was achieved by using the measured photocurrents to control the real and imaginary components of the displacement field using electrically controlled modulators. As the measurement records, the photocurrents, are classical stochastic processes they can be scaled by a gain factor, g, to produce the required β.

The experiment included an additional step to verify to what extent the state received by Bob faithfully reproduced the stat of the client field. In this experiment the state of the client was a coherent state. In essence another party, Victor, is verifying the fidelity of the teleportation using homodyne detection to monitor the quadrature variances of the teleported state.

The key feature that indicates success of the teleportation is a drop in the quadrature noise seen by Victor when Bob applies the appropriate unitary operator to his state. This is done by varying the gain g. If Bob simply does nothing to his state ($g = 0$), then Victor simply gets one half of a squeezed state. Such a state has a quadrature noise level well above the vacuum level of the coherent state. As Bob varies his gain, Victor finds the quadrature noise level fall until, at optimal gain, the teleportation is effected and the variance falls to the vacuum level of a coherent state. In reality of course extra sources of noise introduced in the detectors and control circuits limit the extent to which this can be achieved.

In a perfect system the fidelity should be peaked at unit gain. However photon loss in the shared entanglement resource and detector inefficiencies reduce this. In the experiment, the average fidelity at unit gain was found to be $F = 0.58 \pm 0.002$. As discussed previously, this indicates that entanglement is an essential part of the protocol.

16.4 Quantum Computation*

In 1982 *Richard Feynman* [23] suggested there were certain problems that would be difficult to perform on a computer running according to classical mechanics but which would be easy to do on a computer running according to quantum principles. The reason why this is so is easy to see. A quantum system consisting of say N interacting spins requires a simulation using vectors of 2^N dimensions in general. This exponential growth of the basis size is what makes classical simulations of complex quantum problems so difficult. On the other hand if we built a system with N interacting spins and allowed it to evolve unitarily, no such difficulty would be encountered. It would appear that a computer executing unitary evolution on a system of two level systems could significantly outperform a classical computer set to solve the equivalent problem.

In 1985 David Deutsch [24] showed in more detail what would be required for a quantum computer and gave examples of problems that might be solved more efficiently on such a machine when compared to a classical machine. The promise of quantum computation suggested by Feynman and elaborated by Deutsch was made very apparent in the factoring algorithm of Shor in 1994 [25]. Shor gave a quantum algorithm by which a large integer could be factored into its prime components with high probability, more efficiently than any known algorithm for a classical computer. As the supposed difficulty of factoring large integers is used in modern encryption schemes, Shor's algorithm indicated that such schemes would be open to attack by anyone with a quantum computer.

Quantum computers are as constrained as classical computers in the kinds of functions they can evaluate (so called computable functions) however a quantum computer can potentially solve a problem more efficiently than a classical computer. The efficiency of an algorithm is related to how many computational steps are required to solve the problem as the "size" of the problem increase. The size of a problem can often be expressed by the number of bits in a single number, for example in the case of the factoring problem, the size of the problem is just the number of bits required to store the number to be factored. If the number of steps required to implement an algorithm grows exponentially with the size of the problem, the algorithm is not efficient. If however the number of steps grows only as a polynomial power of the size of the problem, the algorithm is efficient. Shor's algorithm is an efficient factoring algorithm for a quantum computer, while all known algorithms for factoring on a classical computer require an exponentially increasing number of steps as the size of the integer to be factored increases.

How does a quantum computer achieve this enormous increase in efficiency? The answer lies in the quantum superposition principle. Suppose we wish to evaluate a function f on some binary input string x to produce a binary output string, $f(x)$. We can code the input and output binary string as the product state of N qubits. The output qubits however are preset to zero. Now we set up a machine so that under

* This section first appeared in "Springer Handbook of Lasers and Optics" ed. Träger, (Springer, New York, 2007)

unitary quantum evolution the state transforms as

$$|x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle \tag{16.34}$$

Why do we demand that the transformation be unitary? Consider what happens when we prepare the input qubits in a uniform superposition of all possible input states;

$$\sum_x |x\rangle|0\rangle \rightarrow \sum_x |x\rangle|f(x)\rangle \tag{16.35}$$

If the dynamics is unitary the linearity of quantum mechanics ensures that (16.34) implies (16.35). It would appear that in a single run of the machine we have evaluated all possible values of the function.

This is not quite as interesting as it seems. If we measure the output qubits we will get one value at random. That does not seem very useful. To see why it is useful to do this let us ask; when would we ever want to evaluate every value of a particular function? The answer, is when we are not so much interested in a particular value of the function as a *property* of the function. The power of quantum computation arises in what we do next, after the transformation in (16.35). In the next step we continue to unitarily process the output register to extract, in one go, a property of the function, while simultaneously giving up information on the output of any particular evaluation. In all of this we emphasise the need to perform perfect unitary transformations of the qubits. Moreover the unitary transformations necessarily entangle many qubit degrees of freedom. A quantum computer must produce highly entangled states of many qubits without suffering any decoherence. It is this requirement that makes a physical realisation of a quantum computer so difficult to achieve as we shall see below.

How can we use the superposition state in (16.35) to determine properties of functions? To see this consider a function f which maps the binary numbers $\{0,1\}$ to $\{0,1\}$. There must be four such functions, two of which are constant functions with $f(0) = f(1)$, and two have $f(0) \neq f(1)$, so called balanced functions. Suppose now the problem involves determining if a function is balanced or constant. On a classical computer to answer this we need to make two evaluations of the function, $f(0), f(1)$. We would then need to run the computer twice. However a quantum computer can determine this property in only a single run.

Suppose we have two qubits. One qubit will be used to encode the input data and the other qubit, the output qubit, will contain the value of the function after the machine is run. The output qubit is initially set to 0. The machine might then run according to (16.34). However there is a problem with this expression. If f is a constant function we have two distinct input states unitarily transformed to the same output state. Clearly this is not a reversible transformation and thus cannot be implemented unitarily. The problem is easily fixed however by setting up the machine to evolve the states according to

$$|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \tag{16.36}$$

where the addition is defined modulo two and we have allowed all possible settings of both qubits. The unitary transformation which realises this operation has been called the f -controlled NOT gate [26]. The input qubit x is the control qubit while the output qubit y is the target. If the value of f on the control qubit is one, the bit on the target is flipped; thus the name. Every unitary transformation on qubits can be realised as suitable networks of simple one and two qubit gates using primitive gate operations.

The quantum algorithm that solves this problem is a version of a quantum algorithm first proposed by Deutsch. It proceeds as follows. In the first step we prepare the output qubit in the state $|0\rangle - |1\rangle$ (we ignore normalisation in what follows for simplicity). This can be done using a single qubit rotation $|1\rangle \rightarrow |0\rangle - |1\rangle$. Such a rotation is called a Hadamard transformation. In the second step the input qubit is prepared in the 0 state and is then subjected to a Hadamard gate as well, which immediately produces a superposition of the two possible inputs for the function f. In the third step we couple the input and output qubit via the f -controlled NOT gate. The transformation is

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \rightarrow ((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle) \tag{16.37}$$

In the last step we apply a Hadamrd gate to the input qubit so that

$$((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle) \rightarrow (-1)^{f(0)}|f(0) \oplus f(1)\rangle(|0\rangle - |1\rangle) \tag{16.38}$$

Thus the input qubit is in state 0 if f is constant and is in state 1 if f is balanced and measurement of the qubit will determine if the function is balanced or constant with certainty in a single run of the machine.

There is a simple quantum optical realisation of this algorithm based on a Mach-Zehnder interferometer, see Fig. 16.8. The interferometer couples two modes of the field, labeled upper (U) and lower (L). A single photon in the mode-U encodes logical 1 while a single photon in mode-L encodes logical 0. At the input a single photon in mode-U is transformed by the first beam splitter into a superposition state in which it is in either mode-1 or mode-0. If we encode our qubits so that a $|1\rangle$ corresponds to the photon in mode-1 and a $|0\rangle$ corresponds to a photon in mode-0, the first beam splitter performs a Hadamard transformation. Now we insert into

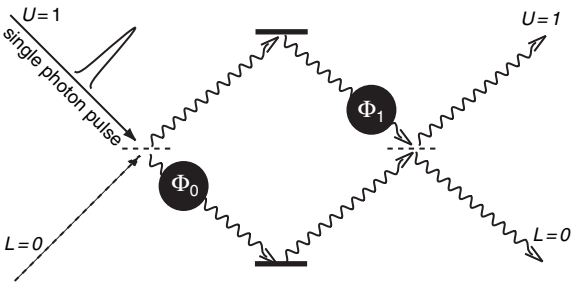

Fig. 16.8 An optical realisation of the Deutsch algorithm in terms of a Mach-Zehnder interferometer. The phase shifts are chosen according to the values of a binary function f as $\phi_0 = f(0)\pi$, $\phi_1 = f(1)\pi$

each arm a phase shift ϕ_i which can only be set at 0 or π phase shift. We encode the value of the functions as $\phi_0 = f(0)\pi,\ \phi_1 = f(1)\pi$. Set the interferometer so that in the absence of the phase shift the photon emerges with certainty at the upper detector, which encodes a 1. The lower detector encodes a zero. It is then clear that if $f(0) = f(1)$ a single photon will emerge at the upper detector, while if $f(0) \neq f(1)$ the photon will be detected at the lower detector, that is the result is a 0.

The previous example illustrates the key features of a quantum algorithm. Firstly it involves unitary transformations of pure quantum states. Secondly we need both single qubit and two qubit interactions to produce entangled states. These were the Hadamard transformation (H-gate) and a controlled NOT transformation (CNOT-gate). It turns out that suitable networks of an arbitrary single qubit rotations, together with a controlled NOT gate, can perform any computation involving arbitrarily many qubits. These features guide us in the search for a suitable physical implementation of a quantum computer. The requirement of unitary is most severe. In general small imperfections in an actual machine will not enable perfect unitary evolution. The pure states are necessarily degraded by unwanted interactions with extraneous degrees of freedom, the environment. The necessity for at least two qubit interactions means we must necessarily seek interactions that entangle at least two quantum systems. Fortunately even in the presence of nonunitary transformations we can use quantum error correction methods to mitigate the deleterious effects of environment induced errors.

16.4.1 Linear Optical Quantum Gates

In the interferometric implementation of Deutsch algorithm we used a simple physical qubit based on a single photon excitation of one of a pair of spatial modes. This is know as a "dual rail" logic. The relationship between logical states and the physical photon number state is

$$|0\rangle_L = |1\rangle_1 \otimes |0\rangle_2 \tag{16.39}$$

$$|1\rangle_L = |0\rangle_1 \otimes |1\rangle_2 \quad . \tag{16.40}$$

The modes could be two input modes to a beam splitter distinguished by the different directions of the wave vector, or they could be distinguished by polarisation. In the case of a beam splitter a single qubit gate is easily implemented by the linear transformation

$$a_i(\theta) = U(\theta)^\dagger a_i U(\theta) \tag{16.41}$$

with $U(\theta) = \exp\left[\theta(a_1 a_2^\dagger - a_1^\dagger a_2)\right]$. Thus

$$a_1(\theta) = \cos\theta a_1 - \sin\theta a_2 \tag{16.42}$$

$$a_2(\theta) = \cos\theta a_2 + \sin\theta a_1 \tag{16.43}$$

The description in the logical basis becomes,

$$|0\rangle_L \rightarrow \cos\theta_1|0\rangle_L - \sin\theta_1|1\rangle_L \tag{16.44}$$
$$|1\rangle_L \rightarrow \cos\theta_1|1\rangle_L + \sin\theta_1|0\rangle_L \tag{16.45}$$

While single qubit gates are readily implemented by linear optical devices such as beam splitters, quarter wave plates, phase shifters etc., two qubit gates are difficult. In order to implement the controlled phase gate (CSIGN) defined by

$$|x\rangle_L|y\rangle_L \rightarrow U_{\rm CP}|x\rangle_L|y\rangle_L = (-1)^{x.y}|x\rangle_L|y\rangle_L \tag{16.46}$$

In a dual rail, single photon code, this can be implemented using a two mode Kerr nonlinearity. A simple nonlinear optical model of a Kerr nonlinearity was discussed in Chap. 5 in relation to optical bistability. The two mode generalisation is described by the Hamiltonian

$$H = \hbar\chi a_1^\dagger a_1 a_2^\dagger a_2 \tag{16.47}$$

At the level of single photons this Hamiltonian produces the transformation, $|x\rangle|y\rangle \rightarrow e^{-ixy\chi t}|x\rangle|y\rangle$ and it is a simple matter to implement the CSIGN gate in the logical basis for the dual rail single photon code.

There are at least two problems in pursuing this approach; (a) the difficulty of realising number states in the laboratory, (b) the difficulty of producing one photon phase shifts of the order of π. We will say more about the fist of these problems below. The second difficulty is very considerable. Third order optical nonlinearities are very small for a field with such a low intensity as a single photon. However experimental advances may eventually overcome this.

A quite different approach to achieve large single photon conditional phase shifts is based on the non-unitary transformation of a state that results when a measurement is made. Consider the situation shown in Fig. 16.9. Two modes of an optical field are coupled via a beam splitter. One mode is assumed to be in the vacuum state (a) or a one photon state (b), while the other mode is arbitrary. A single photon counter is placed in the output port of mode-2. What is the conditional state of mode-1 given a count of n photons?

Consider two modes, a_1, a_2, coupled with a beam splitter interaction, described by the one parameter unitary transformation, given in (16.42 and 16.43) We now assume that photons are counted on mode a_2 and calculate the conditional state

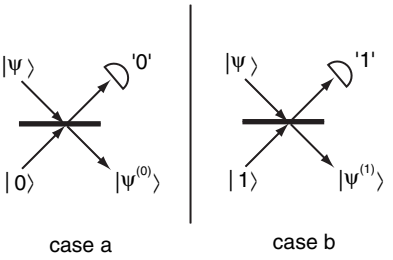

Fig. 16.9 A conditional state transformation conditioned on photon counting measurements

for mode a_1 for two cases: no count and also for a single count at mode a_2. The conditional state of mode a_1 is given by (unnormalised),

$$|\tilde{\psi}^{(i)}\rangle_1 = \hat{\Upsilon}(i)|\psi\rangle_1 \tag{16.48}$$

where

$$\hat{\Upsilon}(i) = {}_2\langle i|U(\theta)|i\rangle_2 \tag{16.49}$$

with $i = 1, 0$. The probability to observe each event is given by

$$P(i) = \langle\psi|\hat{\Upsilon}^\dagger(i)\hat{\Upsilon}(i)|\psi\rangle_1 \tag{16.50}$$

which fixes the normalisation of the state,

$$|\psi^{(i)}\rangle_1 = \frac{1}{\sqrt{P(i)}}|\tilde{\psi}^{(i)}\rangle_1 \tag{16.51}$$

In Exercise 16.5 we find that

$$\hat{\Upsilon}(0) = \sum_{n=0}^{\infty} \frac{(\cos\theta - 1)^n}{n!}(a_1^\dagger)^n a_1^n$$
$$\hat{\Upsilon}(1) = \cos\hat{\Upsilon}^{(0)} - \sin^2\theta a_1^\dagger \hat{\Upsilon}^{(0)} a_1$$

This can be written more succinctly using normal ordering,

$$\hat{\Upsilon}(0) =: e^{\ln(\cos\theta)} : \tag{16.52}$$

In order to see how we can use these kind of transformations to effect a CSIGN gate, consider the situation shown in Fig. 16.10. Three optical modes are mixed on a sequence of three beam splitters with beam splitter parameters θ_i. The *ancilla* modes, a_1, a_2 are restricted to be in the single photon states $|1\rangle_2, |0\rangle_3$ respectively. We will assume that the *signal* mode, a_0, is restricted to have *at most* two photons, thus

$$|\psi\rangle = \alpha|0\rangle_0 + \beta|1\rangle_0 + \gamma|2\rangle_0 \tag{16.53}$$

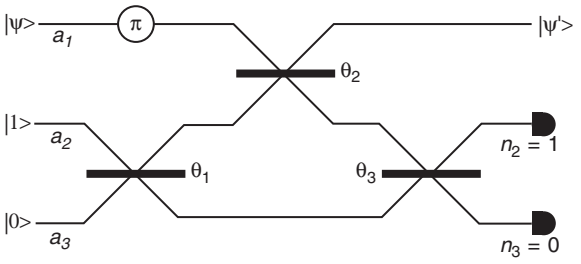

Fig. 16.10 A conditional state transformation on three optical modes, conditioned on photon counting measurements on the ancilla modes a_2, a_3. The signal mode, a_1 is subjected to a π phase shift

This captures the fact that in the dual rail encoding a general two qubit state can have at most two photons. The objective is to chose the beam splitter parameters so that when the two detectors at the output of modes $2,3$ detect $1,0$ photons respectively (that is detect no change in their occupation), the signal state is transformed as

$$|\psi\rangle \rightarrow |\psi'\rangle = \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle \tag{16.54}$$

with a probability that is *independent* of the input state $\psi\rangle$. This last condition is essential as in a quantum computation, the input state to a general two qubit gate is completely unknown. We will call this transformation the NS (for nonlinear sign shift) gate. In Exercise 16.7 we find that this can be achieved using: $\theta_1 = -\theta_3 = 22.5^\circ$ and $\theta_2 = 65.53^\circ$. The probability of the conditioning event ($n_2 = 1, n_3 = 0$) is $1/4$. Note that we can't be sure in a given trial if the correct transformation will be implemented. Such a gate is called a *nondeterministic* gate. However the key point is that success is heralded by the results on the photon counters (assuming ideal operation).

We can now proceed to a CSIGN gate in the dual rail basis. Consider the situation depicted in Fig. 16.11. We first take two dual rail qubits encoding for $|1\rangle_L|1\rangle_L$. The single photon components of each qubit are directed towards a 50/50 beam splitter where they overlap perfectly in space and time. This is precisely the case of the Hong-Ou-Mandel interference discussed in Exercise 3.4(c), and produces a state of the form $|0\rangle_2|2\rangle_3 + |2\rangle_2|0\rangle_3$. We then insert an NS gate into each output arm of the HOM interference. When the conditional gates in each arm work, which occurs with probability $1/16$, the state is multiplied by an overall minus sign. Finally we direct these modes towards another HOM interference. The output state is thus seen to be $-|1\rangle_L|1\rangle_L$. One easily checks the three other cases for the input logical states to see that this device implements the CSIGN gate with a probability of $1/16$ and successful operation is heralded.

Clearly a sequence of nondeterministic gates is not going to be much use: the probability of success after a few steps will be exponentially small. The key idea in using nondeterministic gates for quantum computation is based on the idea of gate teleportation of Gottesmann and Chuang [27]. We saw in Sect. 16.3 that in quantum teleportation an unknown quantum state can be transferred from A to B provided A and B first share an entangled state. Gottesmann and Chuang realised that it is

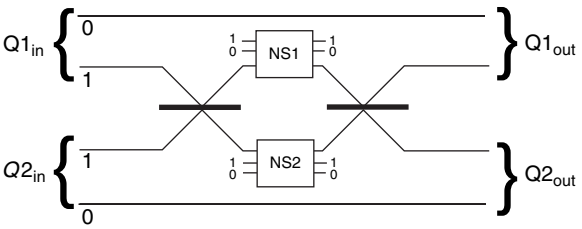

Fig. 16.11 A conditional state transformation conditioned on photon counting measurements. A CSIGN gate that works with probability of 1/16. It uses HOM interference and two NS gates

possible to simultaneously teleport a two qubit quantum state and implement a two qubit gate in the process by first applying the gate to the entangled state that A and B share prior to teleportation.

We use a non deterministic NS gate to prepare the required entangled state, and only complete the teleportation when the this stage is known to work. The teleportation step itself is non deterministic but, as we see below, by using the appropriate entangled resource the teleportation step can be made near deterministic. The near deterministic teleportation protocol requires only photon counting and fast feed-forward. We do not need to make measurements in a Bell basis.

A nondeterministic teleportation measurement is shown in Fig. 16.12. The client state is a one photon state in mode-0 $\alpha|0\rangle_0 + \beta|1\rangle_0$ and we prepare the entangled ancilla state

$$|t_1\rangle_{12} = |01\rangle_{12} + |10\rangle_{12} \tag{16.55}$$

where mode-1 is held by the sender, A, and mode-2 is held by the receiver, B. For simplicity we omit normalisation constants wherever possible. This an ancilla state is easily generated from $|01\rangle_{12}$ by means of a beam splitter.

If the total count is $n_0 + n_1 = 0$ or $n_0 + n_1 = 2$, an affective measurement has been made on the client state and the teleportation has failed. However if $n_0 + n_1 = 1$, which occurs with probability 0.5, teleportation succeeds with the two possible conditional states being

$$\alpha|0\rangle_2 + \beta|1\rangle_2 \text{ if } n_0 = 1, n_1 = 0 \tag{16.56}$$

$$\alpha|0\rangle_2 - \beta|1\rangle_2 \text{ if } n_0 = 0, n_1 = 1 \tag{16.57}$$

This procedure implements a partial Bell measurement and we will refer to it as a nondeterministic teleportation protocol, $\mathbf{T}_{1/2}$. Note that teleportation failure is detected and corresponds to a photon number measurement of the state of the client qubit. Detected number measurements are a very special kind of error and can be easily corrected by a suitable error correction protocol. For further details see [28]

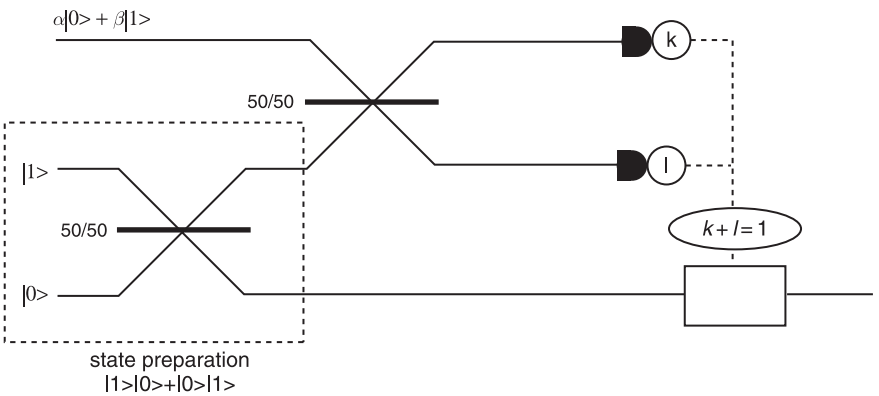

Fig. 16.12 A partial teleportation system for single photons states using a linear optics

The next step is to use $\mathbf{T}_{1/2}$ to effect a conditional sign flip $\text{csign}_{1/4}$ which succeeds with probability $1/4$. Note that to implement csign on two bosonic qubits in modes $1,2$ and $3,4$ respectively, we can first teleport the first modes of each qubit to two new modes (labelled 6 and 8) and then apply csign to the new modes. When using $\mathbf{T}_{1/2}$, we may need to apply a sign correction. Since this commutes with csign, there is nothing preventing us from applying csign to the prepared state before performing the measurements. The implementation is shown in Fig. 16.13 and now consists of first trying to prepare two copies of $|t_1\rangle$ with csign already applied, and then performing two partial Bell measurements. Given the prepared state, the probability of success is $(1/2)^2$. The state can be prepared using $\text{csign}_{1/16}$, which means that the preparation has to be retried an average of 16 times before it is possible to proceed.

To improve the probability of successful teleportation to $1-1/(n+1)$, we generalise the initial entanglement by defining

$$|t_n\rangle_{1\ldots 2n} = \sum_{j=0}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j} \,. \tag{16.58}$$

The notation $|a\rangle^j$ means $|a\rangle|a\rangle\ldots$, j times. The modes are labelled from 1 to $2n$, left to right. Note that the state exists in the space of n bosonic qubits, where the kth qubit is encoded in modes $n+k$ and k (in this order).

To teleport the state $\alpha|0\rangle_0 + \alpha|1\rangle_0$ using $|t_n\rangle_{1\ldots 2n}$ we first couple the client mode to half of the ancilla modes by applying an $n+1$ point Fourier transform on modes 0 to n. This is defined by the mode transformation

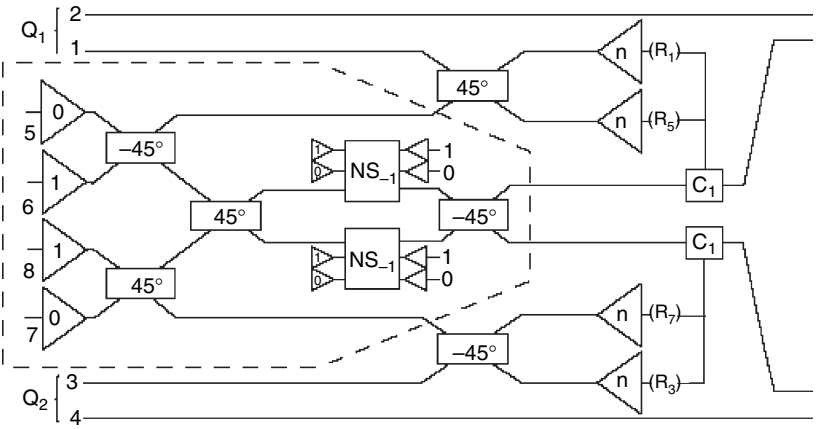

Fig. 16.13 A CSIGN two qubit gate with teleportation to increase success probability to $1/4$. When using the basic teleportation protocol (T1), we may need to apply a sign correction. Since this commutes with CSIGN, it is possible to apply CSIGN to the prepared state before performing the measurements, reducing the implementation of CSIGN to a state-preparation (outlined) and two teleportations. The two teleportation measurements each succeed with probability 1/2, giving a net success probability of 1/4. The correction operations C1 consist of applying the phase shifter when required by the measurement outcomes

$$a_k \rightarrow \frac{1}{\sqrt{n+1}} \sum_{l=0}^{n} \omega^{kl} a_l \tag{16.59}$$

where $\omega = e^{i2\pi/(n+1)}$ This transformation does not change the total photon number and is implementable with passive linear optics. After applying the Fourier transform, we measure the number of photons in each of the modes 0 to n. If the measurement detects k bosons altogether, it is possible to show [28] that if $0 < k < n+1$, then the teleported state appears in mode $n+k$ and only needs to be corrected by applying a phase shift. The modes $2n-l$ are in state 1 for $0 \leq l < (n-k)$ and can be reused in future preparations requiring single bosons. The modes are in state 0 for $n-k < l < n$. If $k = 0$ or $k = n+1$ an effective measurement of the client is made, and the teleportation fails. The probability of these two events is $1/(n+1)$, regardless of the input. Note that again failure is detected and corresponds to measurements in the basis $|0\rangle, |1\rangle$ with the outcome known. Note that both the necessary correction and the receiving mode are unknown until after the measurement.

The linear optics quantum computing (LOQC) model described above can be drastically simplified by adopting the cluster state method of quantum computation [29]. The cluster state model was developed by Raussendorf and Breigel [30] and is quite different from the circuit models that we have been using. In cluster state QC, an array of qubits is initially prepared in a special entangled state. The computation then proceeds by making a sequence of single qubit measurements. Each measurement is made in a basis that depends on prior measurement outcomes. Nielsen realised that the LOQC mode of [28] could be used to efficiently assemble the cluster using the nondeterministic teleportation t_n. As we saw the failure mode of this gate constituted an accidental measurement of the qubit in the computational basis. The key point is that such an error does not destroy the entire assembled cluster but merely detaches one qubit from the cluster. This enables a protocol to be devised that produces a cluster that grows on average. The LOQC cluster state method dramatically reduces the number of optical elements required to implement the original LOQC scheme. Of course if large single photon Kerr nonlinearities were available, the optical cluster state method could be made deterministic [31].

A number of LOQC protocols have been implemented in the laboratory. The first experiment was performed by Pittmann and Franson [32]. This used entangled ancillas that are readily produced as photon pairs in a spontaneous parametric down conversion process. A simplified version of the LOQC model was implemented by O'Brien et al. [33], based on a proposal of Ralph et al. [34] for a CNOT gate shown in Fig. 16.14. The simplification results by firstly setting the beam splitter parameters θ_1, θ_3 to zero in the NS gate implementation and secondly only detecting photon coincidences at the output. This gate performs all the operations of a CNOT gate but requires only a two photon input. Detecting only coincidences means that the device must be configured so that correct operation leads to a coincidence detection of both photons at the output. The gate is non deterministic but gate failures are simply not detected at all. In essence, the control (C) and target (T) qubits act as their own ancilla. When the control is in the logical one state, the control and target photons interfere non-classically at the central $1/3$ beam splitter which causes

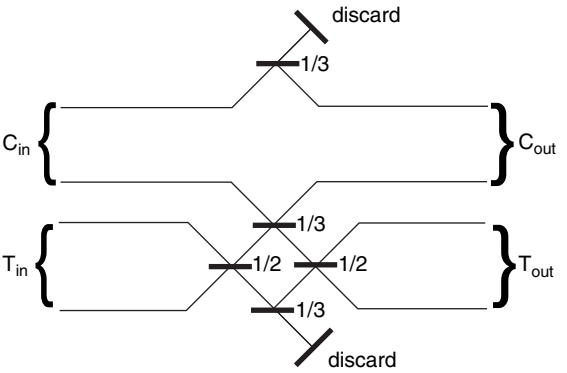

Fig. 16.14 A simplified CNOT gate that gives correct operation only when both input photons are detected coincidentally at the output

a π phase-shift in the upper arm of the central interferometer and the target state qubit is flipped. The qubit value of the control is unchanged. Successful operation is heralded by coincidence detection of both photons and success will occur with probability $1/9$.

In the UQ experiment the two modes of each qubit are distinguished by orthogonal polarisations. This may be converted to spatial mode encoding by using polarising beam splitters and a half wave plate, as shown in Fig. 16.15. The key advantage in using a gate based on two photon coincidence detection is that spontaneous parametric down conversion (SPDC) may be used in place of true single photon sources. An SPDC produces a photon pair in two distinct spatio-temporal modes at random times. There is a small probability of producing more than two photons, but this can be neglected.

The truth table for a CNOT operation was experimentally determined by preparing each of the four possible input states to the gate, $CT\rangle = |00\rangle, |11\rangle, |10\rangle, |01\rangle$. A comparison of the experimental results and the ideal CNOT gate are shown in Fig. 16.14. A single classical interference event is required when the control is in

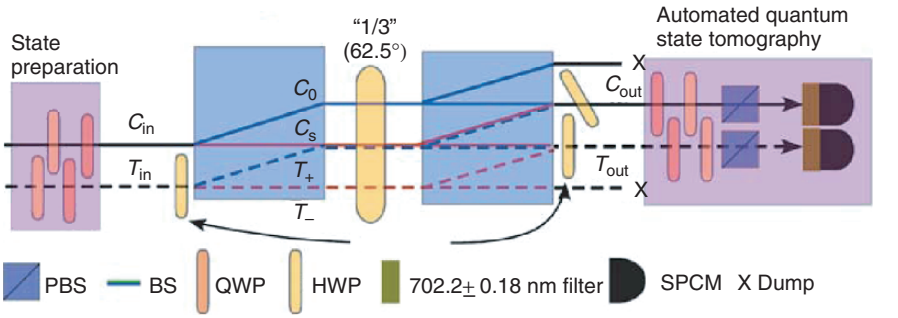

Fig. 16.15 The optical design schematic of the polarisation encoding implementation of the experiment of O'Brien et al., PBS: polarising beam splitter, QWP: quarter wave plate, HWP: half wave plate, SPCM: single photon counting module and X: beam dump. Reproduced, with permission, from Nature, **426**, 264 (2003)

state $|0\rangle_L$ and experimentally the correct output is obtained in roughly 95% of cases. In the case of the control in state $|1\rangle_L$, correct operation is obtained in only 75% of cases as this situation requires a non classical interference event for which very careful mode matching is required.

While this provides good evidence the gate is working the key test of a quantum CNOT gate is that it produce maximally entangled states when the control is in a superposition of the two logical states. For example if the control is in state $|0\rangle_L - |1\rangle_L$, while the target is in $1\rangle_L$, the two-qubit output state is $|\psi^-\rangle = |01\rangle_L - |10\rangle_L$ (where $|xy\rangle_L = |x\rangle_L \otimes |y\rangle_L$, with the first factor the control qubit and the second factor the target). In testing the truth table, the output logical states were measured in the logical basis. Such a "computational basis" measurement of course will not reveal the classical correlation imposed by the truth table but not quantum coherence. To see the quantum coherence implicit in the entangled state we need to measure in a basis other than the computational basis. In the experiment this was done by measuring the coincidence count rate while using a half wave plate set to pass control photons in either of the states $|0\rangle_L$ or state $|0\rangle_L + |1\rangle_L$. The experimental results are show in Fig. 16.16. The visibilities in the two curves are greater than 90% which is the signature of entanglement in the output state.

An even better diagnostic of the gate operation is provided by state tomography, a reconstruction of the full density matrix of the output state [35], when the output is entangled. State tomography requires sampling the statistics for the measurement outcomes of 16 different two qubit projections. Given these statistics data inversion can be devised to reconstruct the density matrix for the output state. Given the density matrix, we can then compute its overlap, or fidelity, with respect to the pure ideal entangled state $|\psi^-\rangle$ that the ideal gate would produce. In the case of $|\psi^-\rangle$ the fidelity obtained in the experiment was 0.87 ± 0.08. This is sufficiently high that such a state were it not destroyed in the detection process, would violate a Bell inequality test.

More recent experiments have improved on these early experiments. An NS gate close to the original proposal, was implemented in the Zeilinger group, using a polarisation encoding and the four photon state emitted by spontaneous parametric down conversion [36]. As in the UQ experiment, a coincidence detection configuration was used to signal correct operation of the gate. The experimentally observed

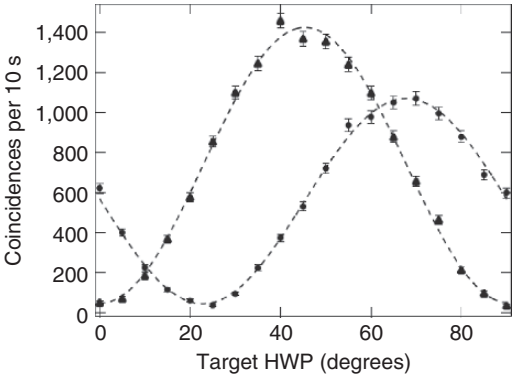

Fig. 16.16 Conditional coincidence rtes for non-orthogonal measurement bases. The control analyser was set to pass $|0\rangle_L + |1\rangle_L$ (*circles*) and $|0\rangle_L$ (*triangles*) when the input to the control is $(|0\rangle_L - |1\rangle_L)$ and the input to the target is $|1\rangle_L$. Reproduced, with permission, from Nature, **426**, 264 (1003)

conditional phase shift was $1.05 \pm 0.06\pi$. Future progress on linear optical quantum computing schemes will most likely be based on cluster state implementations. A four photon cluster state implementation was recently implemented by the Zeilinger group [37].

16.4.2 Single Photon Sources

As we have seen both QKD and LOQC motivate the development of single photon sources. Single photon sources enable QKD to escape beam splitter attacks that are possible with weak coherent pulses. In order to progress to scaleable architectures, LOQC will certainly require the development of good single photons sources and highly efficient single photon detectors that can in fact discriminate between $0, 1$ and 2 photons. Fortunately steady progress is being made on both technologies. The requirements on single photon sources are much more demanding than those for single photon sources in QKD and we now briefly discuss some of these.

What we need is an optical pulse source in which each pulse contains one and only one photon. Clearly such a source is going to produce photon antibunching and the $g^{(2)}(\tau)$ (see Sect. 3.6) is clearly a key diagnostic for such a source. However a more stringent requirement is the ability of such a source to produce a strong Hong-Ou-Mandle interference dip. (See Exercise 3.4(c)).

In order to define single photon states, let us begin by defining the positive frequency field component as,

$$a(t) = \sum_{n=1}^{\infty} a_n \mathrm{e}^{-int} \tag{16.60}$$

The allowed wave vectors for plane wave modes in a box of length L, form a denumerable set given by $k_n = \frac{n\pi}{L}$ with corresponding frequencies $\omega_n = ck_n$. If we measure time in units of $\pi L/c$, the allowed frequencies may simply be denoted by an integer $\omega_n = n = 1, 2, \ldots$. The Bose annihilation and creation operators obey the usual commutation relations. Following the standard theory of photo-detection (see Sect. 3.10) the probability per unit time for detecting a single photon is given by $p_1(t) = \gamma n(t)$ where $n(t) = \langle a^\dagger(t)a(t)\rangle$ and the parameter γ characterises the detector. A single-photon state may be then defined as

$$|1; f\rangle = \sum_{m=1}^{\infty} f_m a_m^\dagger |0\rangle \tag{16.61}$$

where $|0\rangle = \prod_m |0\rangle_m$ is the multimode global vacuum state, and we require that the single photon amplitude, f_m satisfies

$$\sum_{m=0}^{\infty} |f_m|^2 = 1 \tag{16.62}$$

The counting probability is then determined by

$$n(t) = \left| \sum_{k=1}^{\infty} f_k e^{-ikt} \right|^2 \tag{16.63}$$

This function is clearly periodic with a period 2π. As the spectrum is bounded from below by $n = 1$, it is not possible to choose the amplitudes f_n so that the functions $n(t)$ have arbitrarily narrow support on $t \in [0, 2\pi)$.

While a field for which exactly one photon is counted in one counting interval, and zero in all others, is no doubt possible, it does not correspond to a more physical situation in which a source is *periodically* producing pulses with exactly one photons per pulse. To define such a field state we now introduce time-bin operators. For simplicity we assume that only field modes $n \leq N$ are excited and all others are in the vacuum state. It would be more physical to assume only field modes are excited in some band, $\Omega - B \leq n \leq \Omega + B$. Here Ω is the carrier frequency and $2B$ is the bandwidth. However this adds very little to the discussion.
Define the operators

$$\tilde{a}_\nu = \frac{1}{\sqrt{N}} \sum_{m=1}^{N} \mathrm{e}^{-\mathrm{i}\tau m\nu} a_m \tag{16.64}$$

where $\tau = \frac{2\pi}{N}$ This can be inverted to give

$$a_m = \frac{1}{\sqrt{N}} \sum_{\nu=1}^{N} \mathrm{e}^{\mathrm{i}\tau m\nu} \tilde{a}_\nu \tag{16.65}$$

The temporal evolution of the positive frequency components of the field modes then follows from (16.60)

$$a(t) = \sum_{\mu=1}^{N} g_\mu(t) \tilde{a}_\mu \tag{16.66}$$

where

$$g_\mu(t) = \frac{1}{\sqrt{N}} \left[1 - e^{i(\nu\tau - t)} \right]^{-1} \tag{16.67}$$

The time-bin expansion functions, $g_\mu(t)$ are a function of $\nu\tau - t$ alone and are thus simple translations of the functions at $t = 0$. The form of (16.66) is a special case of a more sophisticated way to define time-bin modes. If we were to regard $a(t)$ as a classical signal then the decomposition in (16.66) could be generalised as a wavelet transform where the integer μ labels the translation index for the wavelet functions. In that case the functions $g_\mu(t)$ could be made rather less singular. In an experimental context however the form of the functions $g_\mu(t)$ depends upon the details of the generation process.

The linear relationship between the plane wave modes a_m and the time bin modes $\tilde{a}_\nu$ is realised by a unitary transformation that does not change particle number, so the vacuum state for the time-bin modes is the same as the vacuum state for the global plane wave modes. We can then define a one-photon time-bin state as

$$|\tilde{1}\rangle_\nu = \tilde{a}_\nu^\dagger |0\rangle \tag{16.68}$$

The mean photon number for this state is,

$$n(t) = |g_\nu(t)|^2 \tag{16.69}$$

This function is periodic on $t \in [0, 2\pi)$ and corresponds to a pulse localised in time at $t = \nu\tau$. Thus the integer ν labels the temporal coordinate of the single photon pulse.

We are now in a position to define an N-photon state with one photon per pulse. In addition to the mean photon number, $n(t)$ we can now compute two-time correlation functions such as the second order correlation function, $G^{(2)}(\tau)$ defined by

$$G^{(2)}(T) = \langle a^\dagger(t) a^\dagger(t+T) a(t+T) a(t) \rangle \tag{16.70}$$

The simplest example for $N = 2$ is

$$|1_\mu, 1_\nu\rangle = \tilde{a}_\mu^\dagger \tilde{a}_\nu^\dagger |0\rangle \qquad \mu \neq \nu \tag{16.71}$$

The corresponding mean photon number is

$$n(t) = |g_\mu(t)|^2 + |g_\nu(t)|^2 \tag{16.72}$$

as would be expected. The two-time correlation function is,

$$G^{(2)}(\tau) = |g_\mu(t) g_\nu(t+T) + g_\nu(t) g_\mu(t+T)|^2 \tag{16.73}$$

Clearly this has a zero at $T = 0$ reflecting the fact that the probability to detect a single photon immediately after a single photon detection is zero, as the two pulses are separated in time by $|\mu - \nu|$. This is known as *anti-bunching* and is the first essential diagnostic for a sequence of single photon pulses with one and only one photon per pulse. When $T = |\mu - \nu|\tau$ however there is a peak in the two-time correlation function as expected.

An example of such a single photon source producing a second order two-time correlation function of this kind was implemented by the group of Yamamoto [38]. The source was based on spontaneous emission from exciton recombination from a single InAs quantum dot in a micropillar cavity using distributed Bragg reflecting mirrors. The devices operate at low temperature ($3 - 7$ K) and are pumped by a pulsed TiSi laser with 3 ps pulses every 13 ns. Three quantum dots were reported producing light with wavelengths 931, 932 and 937 nm. In Fig. 16.17 we show the experimental results for the second order two time correlation function using a Hanbury-Brown and Twiss configuration.

We now consider an interferometer with single photon input states. The most relevant example for LOQC protocols is the Hong-Ou-Mandel (HOM) interferometer. This example has been considered by Rohde and Ralph [39]. In this case two fields, distinguished by momentum or polarisation are coupled by a linear optical device (referred to for simplicity as a beam-splitter). After the interaction, each field is

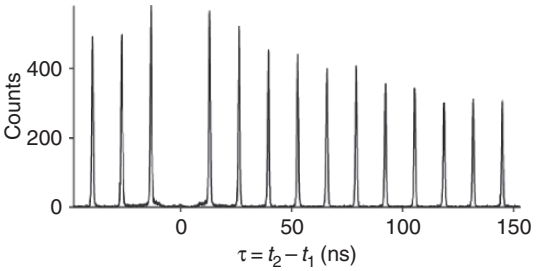

Fig. 16.17 The photon correlation histogram for emission form a single exciton quantum dot. The results were obtained using a Hanbury-Brown and Twiss experiment. The emission from the quantum dot was split into two paths via a beam splitter and each path directed towards a photon detector. The number of events in which a photon was detected on one detector at time t_1 and on the other detector at time $t_2 = t_1 + \tau$. The suppression of the peak at zero delay is characteristic of a single photon pulse source. (From [38]) reproduced with permission from Nature

directed onto a photon counter, and the probability for a coincidence count is determined. We label the two sets of modes by the latin symbols a, b so for example the positive frequency parts of each field are simply $a(t), b(t)$. The coupling between the modes is described by a scattering matrix connecting the input and output plane waves

$$a_n^{\text{out}} = \sqrt{\eta} a_n + \sqrt{1-\eta} b_n \tag{16.74}$$

$$b_n^{\text{out}} = \sqrt{\eta} b_n - \sqrt{1-\eta} a_n \tag{16.75}$$

where $0 \leq \eta \leq 1$. This is realised by a unitary transformation, U, for example, $a_n^{\text{out}} = U^\dagger a_n U$. The total photon number at the input is $N(t) = \langle a^\dagger(t) a(t) \rangle + \langle b^\dagger(t) b(t) \rangle$. It is easy to see that this is unchanged by the beam-splitter transformation. The probability, per unit time, for there to be a coincident detection of a single photon at each output beam is easily seen to be proportional to

$$C = \overline{\langle a^\dagger(t) b^\dagger(t) b(t) a(t) \rangle} \tag{16.76}$$

The overline represents a time average over a detector response time that is long compared to the period of the field carrier frequencies. In this example we only need consider the case of one photon in each of the two distinguished modes, so we take the input state to be

$$|1\rangle_a \otimes |1\rangle_b = \sum_{m,n=1}^{\infty} \alpha_n \beta_m a_n^\dagger b_m^\dagger |0\rangle \tag{16.77}$$

where α_n, β_n refer to the excitation probability amplitudes for modes a_n, b_n respectively. This state is transformed by the unitary transformation, U, to give $|\psi\rangle_{\text{out}} = U|1\rangle_a \otimes |1\rangle_b$. In the case of a 50/50 beam splitter, for which $\eta = 0.5$, this is given as

$$
\begin{aligned}
|\psi\rangle_{out} &= \sum_{n,m=1}^{\infty} \alpha_n \beta_m U a_n^\dagger b_m^\dagger \\
&= \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \beta_m (a_n^\dagger + b_n^\dagger)(b_m^\dagger - a_m^\dagger)|0\rangle \\
&= \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \beta_m [|1\rangle_{a_n}|1\rangle_{b_m} - |1\rangle_{a_n}|1\rangle_{a_m}|0\rangle_b \\
&\quad + |1\rangle_{b_n}|1\rangle_{b_m}|0\rangle_a - |1\rangle_{b_n}|1\rangle_{a_m}]
\end{aligned}
$$

Note that the second and third terms in this sum have no photons in modes b and a respectively. We then have that

$$
C = \frac{1}{2} - \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \alpha_m^* \beta_m \beta_n^* \tag{16.78}
$$

If the excitation probability amplitudes at each frequency are identical, $\alpha_n = \beta_n$ this quantity is zero. In other words only if the two-single photon wave packets are identical do we see a complete cancellation of the coincidence probability. This is the second essential diagnostic for a single photon source. Of course in an experiment complete cancellation is unlikely. The extent to which the coincidence rate approaches zero is a measure of the quality of a single photon source as far as LOQC is concerned. Whether or not this is the case depends on the nature of the single photon source.

In Fig. 16.18 we show the results of a HOM interference experiment using the exciton quantum dot source of Yamamoto [38].

Currently the two schemes used to realise single photon sources are: I conditional spontaneous parametric down conversion, II cavity-QED Raman schemes. As discussed by Rohde and Ralph, type-I corresponds to a Gaussian distribution of α_n as a function of n. The second scheme, type-II, leads to a temporal pulse structure that

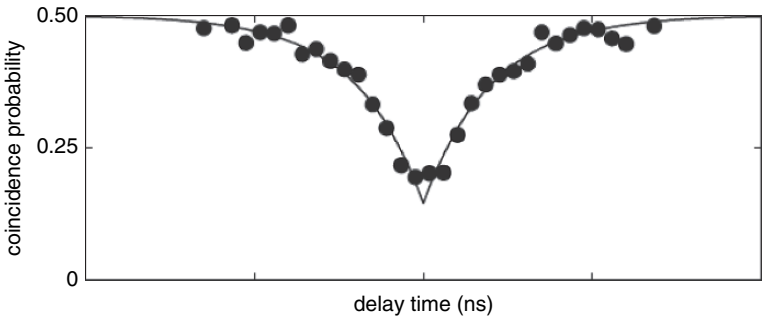

Fig. 16.18 The coincidence count probability for two photons incident on a beam splitter as a function of the time delay in arrival times of the photons at the beam splitter for the exciton quantum dot source of Santori et al. [38]. Reproduced with permission from Nature

is the convolution of the excitation pulse shape and the Lorentzian line shape of a cavity. If the cavity decay time is the longest time in the dynamics, the distribution α_n takes a Lorentzian form.

As an example of the experimental constraints on the generation of single photon states we now review an example of a cavity-QED Raman scheme implemented by Keller et al. [40]. Photon anti-bunching from resonance fluorescence was discussed in Sect. 10.3. If an atom decays spontaneously from an excited to a ground state, a single photon is emitted and a second photon cannot be emitted until the atom is re-excited. Unfortunately the photon is emitted into a dipole radiation pattern over a complete solid angle. Clearly we need to engineer the electromagnetic environment with mirrors, dielectrics, etc, to be sure a preferred mode for emission. However single photon sources based on spontaneous emission are necessarily compromised by the random nature of spontaneous emission. The decay process is a conditional Poison process. This means that after a fast excitation pulse there is a small random time delay in the emission of the photon. This leads to time jitter in the single photon pulse period. A similar situation prevails in the case of single exciton sources [38], where spontaneous recombination leads to time jitter for the same reason. Clearly what we need is a *stimulated* emission process not a spontaneous emission process. A number of schemes based on stimulated Raman emission into a cavity mode have been proposed to this end [40, 41, 42].

Consider a three-level atomic system in Fig. 16.19. The ground state is coupled to the excited state via a two-photon Raman process mediated by a well detuned third level. In this experiment a calcium ion ($^{40}Ca_+$) was trapped in a cavity via an rf ion trap. The cavity field is nearly resonant with the $4^2P_{1/2} \rightarrow 3^2D_{3/2}$ transition. Initially there is no photon in the cavity. An external laser is directed onto the ion and is nearly resonant with the $4^2P_{1/2} \rightarrow 4^2P_{1/2}$ transition. When this laser is on, the atom can be excited to the $3^2D_{3/2}$ level by absorbing one pump photon and *emitting* one photon into the cavity. This is a stimulated Raman process and thus time of emission of the photon into the cavity is completely controlled by the temporal structure of the pump pulse. The photon in the cavity then decays through the end mirror, again as a Poisson process this time at a rate given by the cavity decay rate. This can be made very fast.

In principle one can now calculate the probability per unit time to detect a single photon emitted from the cavity. If we assume every photon emitted is detected, this

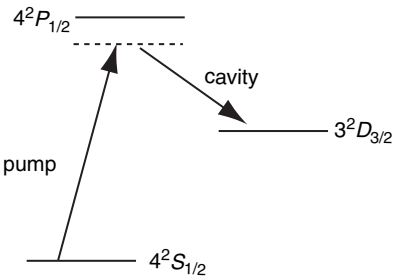

Fig. 16.19 A possible three-level atomic system for a two-photon Raman single photon source. The pump beam is a strong classical coherent pulse. The cavity field is an intracavity field mode initially prepared in a vacuum state

probability is simply $p_1(t) = \kappa\langle a^\dagger(t)a(t)\rangle$ where κ is the cavity decay rate and $a, a^\dagger$ are the annihilation and creation operators for the *intracavity* field and

$$\langle a^\dagger(t)a(t)\rangle = \mathrm{tr}(\rho(t)a^\dagger a) \tag{16.79}$$

where $\rho(t)$ is the total density operator for ion-plus-cavity-field system. This may be obtained by solving a master equation describing the interaction of the electronic states of the ion and the two fields, one of which is the time dependent pump. Of course for a general time-dependent pump pulse-shape this can only be done numerically. Indeed by carefully controlling the pump pulse shape considerable control over the temporal structure of the single photon detection probability may be achieved. In the experiment of *Keller* et al. [40] the length of the pump pulse was controlled to optimise the single photon output rate. The efficiency of emission was found to be about 8%, that is to say, 92% of pump pulses did not lead to a single-photon detection event. This was in accordance with the theoretical simulations. These photons are probably lost through the sides of the cavity. It is important to note that this kind of loss does not effect the temporal mode structure of the emitted (and detected) photons.

In a similar way we can compute the second order correlation function via

$$G^{(2)}(T) = \kappa^2\mathrm{tr}(a^\dagger a e^{\mathscr{L}T}(a\rho(t)a^\dagger) \tag{16.80}$$

where $e^{\mathscr{L}T}$ is a formal specification of the solution to the master equation for a time T after the "initial" conditional state $a\rho(t)a^\dagger$. Once again, due to the non stationary nature of the problem, this must be computed numerically. However if the pump pulse duration is very short compared to the cavity decay time and further the cavity decay time is the fastest decay constant in the system, the probability amplitude to excite a single photon in a frequency at frequency ω is very close to Lorentzian. The experiment of Keller et al. [40] revealed a clear suppression of the peak at $T = 0$ in the (normalised) correlation function $g^{(2)}(T)$, thus passing the first test of a good single photon source.

A very different approach to single photon sources is based on the spontaneous parametric down conversion using a crystal with a significant second order optical non linearity. In these systems, a pair of photons is produced simultaneously, but at random times. However if we detect one photon of the pair in a given time window, we know the temporal coordinates of the other photon. A detailed study of the mode structure of the conditional photon pulse has been undertaken by Walmsley and co-workers [43]. To a very good approximation the probability amplitude functions, α_ω, are Gaussian with variance depending ultimately on the filters used in the conditioning detection step. These sources have been the sources of choice for the early implementations of LOQC. However the random time of pair production means that the single photons are heralded but not produced on-demand. An ingenious scheme to overcome this limitation is being pursued by the NIST group of Migdall [44]. In their scheme a large number of conditional sources are multiplexed, together with fast electro-optical switching, so that at some repetition rate and detection bandwidth, there is near determinant sequence of singe photon detection events.

Exercises

16.1 Consider the following EPR entangled state of two modes A and B,

$$|X,Y\rangle_{AB} = \mathrm{e}^{-\frac{i}{2}\hat{Y}_A\hat{X}_B}|X\rangle_A \otimes |Y\rangle_B \tag{16.81}$$

where the states appearing on the left hand side of this equation are the quadrature phase eigenstates. Verify that this state is a simultaneous eigenstate of $\hat{X}_A - \hat{X}_B$ and $\hat{Y}_A + \hat{Y}_B$ with respective eigenvalues, X, Y.

16.2 The two-mode squeezed vacuum state, (16.16), is also entangled with respect to the correlation specified by the statement: *an equal number of photons in each mode*. However it is not a perfectly entangled state, which would require the (unphysical) case of a uniform distribution over correlated states. Show that the state is an eigenstate of the photon number difference and the phase sum. To show this compute the canonical joint phase distribution $P(\phi_A, \phi_B)$, for the two modes using the projection operator valued measure (see Sect. 2.8). Show that as $\lambda \to 1$ this distribution becomes very sharply peaked at $\phi_A = -\phi_B$. Thus the photon number in each mode are perfectly correlated while the phase in each mode is highly anti correlated.

16.3 Joint quadrature phase measurement of $\hat{X}_C - \hat{X}_A$ and $\hat{Y}_C + \hat{Y}_A$ are made on two modes, A and C, with the results X, Y respectively. Show that the conditional state resulting from this joint quadrature measurement is described by the projection onto the state $|X,Y\rangle_{CA}$ where

$$|X,Y\rangle_{CA} = \mathrm{e}^{-\frac{i}{2}\hat{X}_A\hat{Y}_C}|X\rangle_C \otimes |Y\rangle_A \tag{16.82}$$

16.4 In the protocol for teleportation based on the state in Exercise 16.1, let the total input state for the teleportation protocol be

$$|\psi\rangle_{\mathrm{in}} = |\psi\rangle_C \otimes |X_0, Y_0\rangle_{AB} \tag{16.83}$$

Joint quadrature phase measurements of $\hat{X}_C - \hat{X}_A$ and $\hat{Y}_C + \hat{Y}_A$ are made on the client and sender modes C and A, yielding two real numbers, X, Y respectively. Show that the conditional state of mode B after the measurement on sender and the client, in the special case of $X_0 = Y_0 = 0$, is then given by

$$|\phi^{(X,Y)}\rangle_B = e^{\frac{i}{2}XY} e^{\frac{i}{2}X\hat{Y}_B} e^{-\frac{i}{2}Y\hat{X}_B}|\psi\rangle_B \tag{16.84}$$

16.5 Consider the beam splitter unitary transformation $U = e^{\theta(a_2^\dagger a_1 - a_2 a_1^\dagger)}$. Show that

$$\begin{aligned} {}_2\langle 0|U(\theta)|0\rangle_2 &= \sum_{n=0}^{\infty} \frac{(\cos\theta - 1)^n}{n!}(a_1^\dagger)^n a_1^n \\ {}_2\langle 1|U(\theta)|1\rangle_2 &= \cos\hat{\Upsilon}^{(0)} - \sin^2\theta a_1^\dagger \hat{\Upsilon}^{(0)} a_1 \end{aligned}$$

16.6 A linear optical device acting on N modes may be described by a unitary transformation of the form

$$U(H) = \exp[-i\vec{a}^{\dagger} H \vec{a}] \tag{16.85}$$

where

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \\ a_N \\ \vdots \\ a_N \end{pmatrix} \tag{16.86}$$

and H is a hermitian matrix. Show that this transformation leaves the total photon number invariant,

$$U^{\dagger}(H)\vec{a}^{\dagger} \cdot \vec{a} U(H) = \vec{a}^{\dagger} \cdot \vec{a} \tag{16.87}$$

and induces a linear unitary transformation on the vector $\vec{a}$ as

$$U^{\dagger}(H)\vec{a}U(H) = S(H)\vec{a} \tag{16.88}$$

16.7 Consider the three mode optical device shown in Fig. 16.10. Mode a_1 is the signal mode prepared in an arbitrary two photon state $|\psi\rangle$. Modes a_2, a_3 are ancilla modes prepared in the photon number states $|1\rangle_2$ and $|0\rangle_3$, respectively. Using the notation of Exercise 16.6, let the $S(H)$ be the orthogonal matrix with matrix elements s_{ij}. Show that the (unormalised) conditional state of the signal mode, conditioned on counting one photon on mode a_2 and no photons in mode a_3 is given by $|upsi'\rangle = \hat{E}|\psi\rangle$ with $\hat{E} = s_{22}\hat{A} + s_{12}s_{21}a_1^{\dagger}\hat{A}a_1$ where $\hat{A} = \sum_{n=0}^{\infty} \frac{(s_{11}-1)^n}{n!}(a_1^{\dagger})^n a_1^n$. Verify that, for the choice given in Fig. 16.10, this implements a conditional sign shift gate with probability of 0.25 .

References

1. C.E. Shannon: Bell System. Tech. J. **27**, 379 (1948); Reprinted in, C.E. Shannon, W. Weaver: *The Mathematical Theory fo Communication* (The University of Illinois Press, Urbana 1949)
2. R.B. Ash: *Information Theory* (Dover, New York 1965)
3. Charles H. Bennett 1, David P. DiVincenzo 1, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, William K. Wootters: *Quantum Nonlocality Without Entanglement*, quant- ph/ 9804053 v4 2 Nov 1998

4. A. Peres: Phys. Rev. Lett **77**, 1413 (1996)
5. G. Adesso, F. Illuminati: Phys. Rev. A **72**, 032334 (2005)
6. I. Bengtsson, K. Życzkowski, "Geometry of Quantum States", pp. 333, Cambridge University press (Cambridge, 2006)
7. S. Wiesner: "Conjugate Coding," SIGACT News **15**, 78 (1983)
8. C.H. Bennett, G. Brassard: "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (New York, IEEE 1984)
9. C.H. Bennett, G. Brassard: "The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working," SIGACT NEWS **20** (4), 78 (1989); C.H. Bennett et al.: Experimental Quantum Cryptography, J. Crypto. **5**, 3 (1992)
10. A. Muller, J. Breguet, N. Gisin: Europhys. Lett. **23**, 383 (1993)
11. A.K. Ekert: Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991)
12. C.H. Bennett: Quantum Cryptography Using Any Two Non-Orthogonal States, Phys. Rev. Lett. **68**, 3121 (1992)
13. W.K. Wootters, W.H. Zurek: Nature **299**, 802 (1982); D. Dieks: Phys. Let. A, **92**, 271 (1982)
14. R.J. Hughes, W.T. Buttler, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, C.M. Simmons: Proc. SPIE **3076**, 2 (1997)
15. P.A. Hiskett et al., New Journal of Physics, **8**, 193 (2006)
16. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K. Wooters: Phys. Rev. Lett. **70**, 1895 (1993)
17. B. Schumaker: Phys. Rev. A **51**, 2783 (1995)
18. A. Furasawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzik: Science, **282**, 23 October, 706, (1998)
19. S.L. Braunstein, H.J. Kimble: Phys. Rev. Letts. **80**, 869 (1998)
20. L. Vaidman: Phys. Rev. A **49** 1473 (1994)
21. refer to di Martini teleportation experiment
22. refer to Zeilinger teleportation experiment
23. Richard P. Feynman: *Simulating Physics with Computers*, Int. J. Theoretical Phys., **21**, 467 (1982)
24. D. Deutsch: Quantum-Theory, the Church-Turing Principle and the Universal Quantum Computer. Proc. R. Soc. Lond. A **400**, 97–117 (1985)
25. P. Shor: Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proc. 35th Annual Symposium on Foundations of Computer Science (1994). See also LANL preprint quant-ph/9508027
26. Richard Cleve, Artur Ekert, Leah Henderson, Chiara Macchiavello and Michele Mosca: On quantum algorithms, Complexity, **4**, 33 (1999)
27. D. Gottesman, I.L. Chuang: Nature, **402**, 390–393 (1999)
28. E. Knill, R. Laflamme, G.J. Milburn: Nature, **409**, 46, (2001)
29. Michael A. Nielsen: Phys. Rev. Lett. **93**, 040503 (2004)
30. R. Raussendorf, H.J. Briegel: Phys. Rev. Lett. **86**, 5188 (2001)
31. G.D. Hutchinson, G.J. Milburn: J. Mod. Opt. **51**, 1211–1222 (2004)
32. T.B. Pittman, B.C. Jacobs, J.D. Franson: Phys. Rev. A **64**, 062311 (2001)
33. J.L. OBrien, G.J. Pryde, A.G. White, T.C. Ralph, D. Branning: Nature, **426**, 264 (2003)
34. T.C. Ralph, N.K. Langford, T.B. Bell, A.G. White: Phys. Rev. A **65**, 062324 (2002)
35. D.F.W. James, P.G. Kwiat, W.G. Munro, A.G. White: Phys. Rev. A**64**, 052312 (2001)
36. K. Sanaka,T. Jennewein, Jian-Wei Pan, K. Resch, A. Zeilinger: Phys. Rev. Lett. **92**, 017902–1 (2004)
37. P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, A. Zeilinger: Nature, **434**, 169 (2005)
38. C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, Y. Yamamoto: Nature, **419**, 594, (2002)
39. P.P. Rohde, T.C. Ralph: PRA **71**, 032320 (2005)
40. M. Keller, B. Lange, K. Hayasaka, W. Lange, H. Walther: Nature, **431**, 1075 (2003)
41. M. Hennrich, T. Legero, A. Kuhn, G. Rempe: New J. Phys. **6**, 86 (2004)

42. Christian Maurer, C. Becher, C.s Russo, J. Eschner, R. Blatt: New J. Phys. **6**, 94(2004)
43. W.P. Grice et al.: Physical Review A, **64**, 063815 (2001)
44. A.L. Migdall, D. Branning, S. Castelletto, M. Ware: SPIE Free-Space Laser Communication and Laser Imaging II. To Appear in the Proceeding of SPIE Free-Space Laser Communication and Laser Imaging II, Proc. of the SPIE, **4821**, 455–465, 2002

Further Reading

Nielsen M., I. Chuang: *Quantum Computation and Quantum Information* (Cambridge University press, Cambridge 2000)

Bouuwmester D., A. Ekert, A. Zeilinger: (eds) *The Physics of Quantum Information* (Springer, Berlin 2000)

Hoi-Kwong Lo, Tim Spiller, Sandu Popescu: *Introduction to Quantum Computation and Information* (World Scientific, Singapore 1998)

Loepp S., W.K. Wootters: *Protecting Information: From Classical Error Correction to Quantum Cryptography* (Cambridge University Press, New York 2006)

Gisin N., G. Ribordy, W. Tittel H. Zbinden: *Quantum Cryptography* Rev. Mod. Phys. **74**, 145 (2002)