Quantum interference: experiments and applications

J. G. Rarity and P. R. Tapster

Email alerting service	Receive free email alerts when new articles cite this article - sign up in the box at the top right-hand corner of the article or click **here**

To subscribe to *Phil. Trans. R. Soc. Lond. A* go to: **http://rsta.royalsocietypublishing.org/subscriptions**

Quantum interference: experiments and applications

BY J. G. RARITY AND P. R. TAPSTER

Defence Research Agency, St Andrews Road, Malvern WR14 3PS, UK

We describe the simplest single-photon encoding schemes and introduce the concept of a quantum optical gate. These gates can be used to build up arbitrary entangled states of many initially separate single photons. Experimental realization of such a gate involves the development of nonlinear phase shift elements sensitive at the single quantum level. We report our experimental efforts using linear optical elements and non-classical sources where we are able to demonstrate interference and entanglement of initally separate single-photon pulses.

1. Introduction

In the early part of this century it was realized that light (and matter) will show both wave and particle natures that are inextricably linked in the uncertainty relations of quantum mechanics. In the following 90 years a variety of experiments have been carried out to demonstrate this wave–particle duality both with light (for examples see Taylor 1909; Grangier *et al.* 1987) and recently with atoms (Carnal & Mlynek 1991). Until the mid 1980s, most work was aimed at confirming the physics of single particle interference phenomena. Now it has been exploited in quantum cryptography, a method for establishing identical random numbers (keys) at two locations with absolute security (Bennett *et al.* 1992; Townsend 1994; Rarity *et al.* 1994). In this simple quantum processor, single bits of information are coded onto at most one photon using polarization or interference. A more general quantum processor would build up a many particle entangled state from an initial product state containing several separate particles. In §2 we introduce the concept of encoding information on single photons and describe an optical implementation of a universal quantum optical gate (Barenco 1994). Using such a gate it is possible to entangle the state of a control photon (bit) with that of a target photon (bit). With an assembly of such gates it is possible to construct any arbitrary N-particle entangled state. More specifically, when we associate the state of each output photon with a bit of information, one can perform arbitrary computations. For some specific problems (factorization for example, Shor 1994), such a quantum computer can out-perform a classical computer.

To build a universal quantum gate one needs an ideal Kerr medium showing a significant phase shift conditional on the presence of a single photon. Although this is being approached in some laboratories (see the contribution by Kimble *et al.*), it is not yet an off-the-shelf commodity. In our experiments (§3), we are limited to linear elements and thus address the the fundamental question: 'can one take initially separate particles and interferometrically entangle them?' The simplest way of entangling

Phil. Trans. R. Soc. Lond. A (1997) **355**, 2267–2277

Printed in Great Britain　　　　　　　　　　2267

separate particles is to overlap them at a beam splitter in such a way that they appear indistinguishable when viewed from the beam splitters outputs (§ 3 *a*). The probability amplitude for particles appearing at separate output ports shows full destructive interference and photons leave the beam splitter in pairs (Fearn & Loudon 1987). This effect cannot be reproduced using any classical models. We briefly review the result of the first such experiment carried out with, in principle, separate sources (Rarity & Tapster 1997). Although the interference effect seen provides evidence of entanglement of the two particles, it does not allow tests of the standard Bell inequalities (Bell 1964). We describe simple extensions of the apparatus that allow us to selectively study two- (§ 3 *b*) and three-particle (§ 3 *c*) entanglement and the resulting non-local interference phenomena. In principle, these experiments could be extended to demonstrate entanglement of many (greater than three) separate particles, but we are limited by the low efficiencies of both sources and detectors.

2. One-photon interference and encoding

Take a symmetric Mach–Zehnder interferometer as shown in figure 1. In a simple classical analysis with an input field E_{a0} and associated intensity $I_{a0} = |E_{a0}|^2$, the output intensity will vary as

$$I_{b0/b1} = |E_{b0/b1}|^2 = \tfrac{1}{2}I_{a0}(1 \pm \cos \phi). \tag{2.1}$$

This is a linear loss free device as $I_{b0} + I_{b1} = I_{a0}$ for all interferometer phase differences ϕ. Here we are interested in the behaviour of a single quantum incident on the same interferometer. We associate probability amplitudes with the presence of a photon in the input modes and deal with the probability amplitudes in a similar way to the classical fields. In the simplest case, the photon is input from one mode ($a0$, say) and representented by the number state $|1\rangle_{a0}$ with unit amplitude. This state is transformed at the first beam splitter

$$|1\rangle_{a0} \to (1/\sqrt{2})[|1\rangle_{m0} + \mathrm{i}|1\rangle_{m1}], \tag{2.2}$$

noting that the reflection and transmission amplitudes of the beam splitter are $\mathrm{i}/\sqrt{2}$, $1/\sqrt{2}$ with the phase change on reflection required for energy conservation. Obviously, the presence of the photon in one arm implies an empty mode or vacuum state in the other. In this work we specialize to single-photon states throughout and thus leave the vacuum implicit. After propagating and incurring a phase delay $\mathrm{e}^{\mathrm{i}\phi}$ only in the $m1$ arm of the interferometer, a similar transformation occurs at the second beam splitter and the state becomes

$$|1\rangle_{a0} \to \tfrac{1}{2}\mathrm{i}(1 + \mathrm{e}^{\mathrm{i}\phi})|1\rangle_{b0} + \tfrac{1}{2}(1 - \mathrm{e}^{\mathrm{i}\phi})|1\rangle_{b1}. \tag{2.3}$$

We now identify the probability of detecting a single photon at a particular interferometer output as the modulus square of the associated probability amplitude

$$P_{b0/b1} = \tfrac{1}{2}(1 \pm \cos \phi), \tag{2.4}$$

which, of course, is indentical to the classical result when we have unit intensity input. Again, we see that $P_{b0} + P_{b1} \equiv 1$, i.e. the total probability of detecting a photon is unity in this loss free case.

We can now use this system to encode information on a single photon. A phase $\phi = 0$ sends all photons to $b0$, while $\phi = \pi$ sends all photons to $b1$. We can interpret a detection in $b0$ as a 'zero' and $b1$ as a 'one'. One extension from any classical
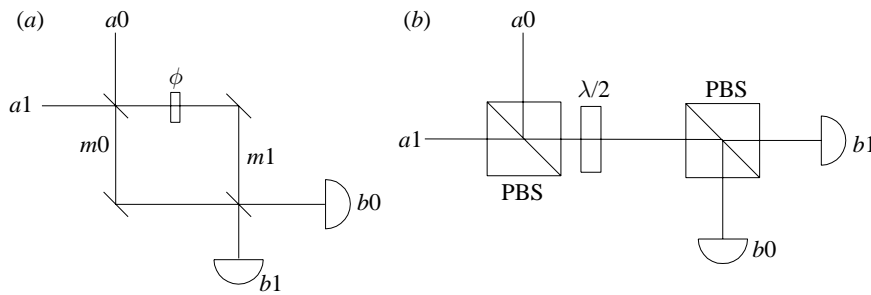
Figure 1. (*a*) Generic Mach–Zehnder interferometer consisting of two 50/50 beam splitters (BS). Input modes are labelled $a0$ and $a1$ and output modes $b0$ and $b1$. The two paths ($m0$, $m1$) through the interferometer are assumed to be identical optical length apart from a phase shift ϕ. (*b*) Polarization interferometer. Here the modes within the interferometer are colinear but correspond to orthogonal circular polarizations. The phase shift ϕ is now varied by rotating a waveplate ($\frac{1}{2}\lambda$).

encoding scheme is the situation where the phase lies between these two extremes. Setting $\phi = \frac{1}{2}\pi$ transforms the input state to

$$|1\rangle_{a0} \to (\mathrm{e}^{3\mathrm{i}\pi/4}/\surd 2)(|1\rangle_{b0} + |1\rangle_{b1}) \tag{2.5}$$

and now our single-photon data is in a superposition state of a 1 and a zero. Detection at this point will provide random information as we have a 50% chance of detecting a one or a zero.

Information can also be coded on a single photon using two orthogonal polarizations such as vertical and horizontal. The coding can be manipulated simply by rotating the polarization in a waveplate. We show this to be equivalent to the above scheme by drawing a polarization interferometer in figure 1*b*. Now the $m0$, $m1$ modes are colinear circularly polarized modes and the relative phase between them is varied by rotating the waveplate. If we define θ as the angle between the waveplate fast axis and the polarization direction of the $a0$ mode, then the interferometer transforms

$$|1\rangle_{a0} \to (\cos 2\theta|1\rangle_{b0} - \sin 2\theta|1\rangle_{b1}) \tag{2.6}$$

and again we see definite outputs when $2\theta = 0, \frac{1}{2}\pi$ and superposition states otherwise.

A direct application of this simple single-photon coding has been in secure key sharing schemes commonly known as quantum cryptography (Bennett *et al.* 1992; Townsend *et al.* 1993; Townsend 1994; Rarity *et al.* 1994). In polarization based quantum cryptography, zeros are encoded with either 0° OR 45° polarized single photons and ones are encoded in 90° OR 135° polarized single photons. The receiver is a polarising beam splitter randomly switched between 0° and 45° measurement bases. The security against eavesdroppers is guaranteed because the coding basis used is not known at the time of transmission and is only shared between sender and receiver (using a conventional communication channel) for those photons that are received.

Returning to the interferometric scheme of figure 1*a*, we see that in general the single-photon input is a superposition state with transformation

$$\alpha|1\rangle_{a0} + \beta|1\rangle_{a1} \to [\mathrm{i}\alpha\cos(\tfrac{1}{2}\phi) + \beta\sin(\tfrac{1}{2}\phi)]|1\rangle_{b0} + [\mathrm{i}\beta\cos(\tfrac{1}{2}\phi) - \alpha\sin(\tfrac{1}{2}\phi)]|1\rangle_{b1}, \tag{2.7}$$

with $\alpha^2 + \beta^2 = 1$ to normalize the one-photon probability and ignoring global phase shifts. The interferometer can be configured in two extreme positions by choosing

$\phi = 0$ and $\phi = \pi$. In the former, all inputs are unchanged after the gate, while the latter acts as a 'quantum' NOT gate. All inputs to $a0$ appear in the $b1$ output and vica versa.

We can extend the simple classically controlled gate above to a fully quantum controlled entity by assuming the phase difference $\phi \equiv \pi$ is conditional on the presence of a photon in an ideal nonlinear medium, as illustrated in figure 2. The control photon is assumed itself to be in a superpostion state between two modes $\delta|1\rangle_{c0} + \gamma|1\rangle_{c1}$ and $\delta^2 + \gamma^2 = 1$. This quantum controlled NOT gate transforms the input product state

$$(\alpha|1\rangle_{a0} + \beta|1\rangle_{a1})(\delta|1\rangle_{c0} + \gamma|1\rangle_{c1}) \rightarrow \alpha[i\delta|1\rangle_{b0}|1\rangle_{c0} - \gamma|1\rangle_{b1}|1\rangle_{c1}]$$
$$+ \beta[i\delta|1\rangle_{b1}|1\rangle_{c0} + \gamma|1\rangle_{b0}|1\rangle_{c1}]. \quad (2.8)$$

The above state cannot be separated into a product state of localized single photons and thus cannot be reproduced classically. The non-local nature of this state is emphasized when we take the simple case of a single photon at the $a0$ input $|1\rangle_{a0}$ and a control photon in an equal superposition $(1/\sqrt{2})(|1\rangle_{c0} + |1\rangle_{c1})$. The state after the gate and after the b and c modes have propagated to remote locations is

$$\Psi_{\text{out}} = (1/\sqrt{2})[i|1\rangle_{b0}|1\rangle_{c0} - \exp i(\theta_b + \theta_c)|1\rangle_{b1}|1\rangle_{c1}], \quad (2.9)$$

with arbitrary propagation phase differences $\theta_{b,c}$. This is the simplest two-photon entangled state and we will discuss non-local interference phenomena associated with such a state in §3b. It is easier to describe the operation of this gate in terms of a matrix transformation as one would with classical logic. The intial (two-bit) state can be represented by four-dimensional vectors $\Psi_{\text{in}} = (I_{00}, I_{01}, I_{10}, I_{11})$ and the final state $\Psi_{\text{out}} = (F_{00}, \ldots, F_{11})$, with elements representing the probability amplitudes for each of the possible input and output states (for example, I_{00} is the probability amplitude for $|1\rangle_{c0}|1\rangle_{a0}$). The gate operation can then be written as a 4×4 matrix transformation,

$$\begin{pmatrix} F_{00} \\ F_{01} \\ F_{10} \\ F_{11} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(\frac{1}{2}\phi) & i\sin(\frac{1}{2}\phi) \\ 0 & 0 & i\sin(\frac{1}{2}\phi) & \cos(\frac{1}{2}\phi) \end{pmatrix} \begin{pmatrix} I_{00} \\ I_{01} \\ I_{10} \\ I_{11} \end{pmatrix}. \quad (2.10)$$

The phase shifts in the beam splitters and internal to the interferometer have been arranged such that the phase shift is zero when the control photons are in the $c0$ mode. The above general operation can be cascaded to link many individual particles in a general entangled state. In principle, this would allow arbitrary algorithms to be carried out. The most spectacular example of such an algorithm was recently reported by Shor (1994). His algorithm is capable of factoring large numbers in a time which increases polynomially with increasing number of digits. The most efficient classical algorithms are limited to an exponential increase in computing time.

3. Interference and entanglement of separate sources

(a) Mixing separate photons at a beam splitter

The operation of arbitrary quantum logic requires the development of effective nonlinear media showing conditional phase shifts of up to π per photon. Although
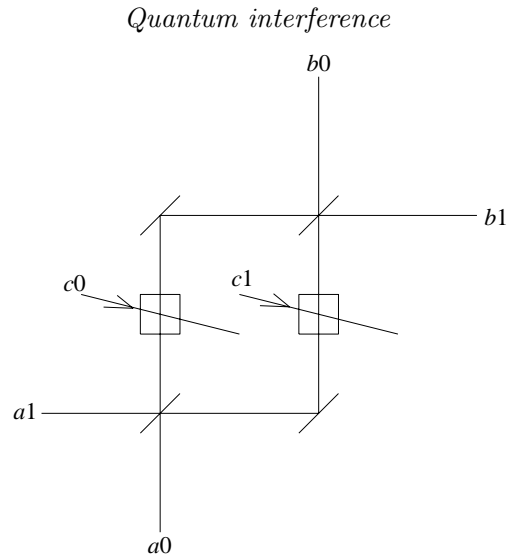
Figure 2. A universal quantum gate. In general, a single-photon input is in a superposition of modes $a0$ and $a1$ and the output (single photon) is in a superposition of modes $b0$ and $b1$. The phase shift within the symmetric Mach–Zehnder interferometer is conditional on the presence of a single photon in either mode $c0$ (phase shift $\phi = 0$) OR in mode $c1$ (phase shift $\phi = \pi$). When the control photon is in a superposition state, the control and output photons are entangled as described in the text.
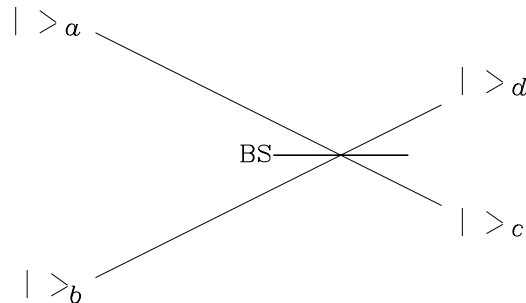

Figure 3. The input (a, b) and output (c, d) modes of a beam splitter (BS). Coincidences are measured between photon counting detectors placed in the c and d modes.

this is being approached in some laboratories (Tourchette *et al.* 1995), the universal quantum gate is still some way off. We are still interested in building a variety of entangled states in the laboratory and find that we can go some way simply using the humble beam splitter.

The beam splitter is represented as in figure 1 with input modes $|\ \rangle_a$, $|\ \rangle_b$ and output modes $|\ \rangle_c$, $|\ \rangle_d$. We again assume equal transmission and reflection amplitudes $t = 1/\sqrt{2}$, $r = \mathrm{i}/\sqrt{2}$. An input state containing two single-photon states in a product state is transformed by the beam splitter to give

$$|1\rangle_a|1\rangle_b \rightarrow [(t^2 + r^2)|1\rangle_c|1\rangle_d + \mathrm{i}rt(|2\rangle_c|0\rangle_d + |0\rangle_c|2\rangle_d)]. \tag{3.1}$$

The amplitude for seeing $|1\rangle_c|1\rangle_d$ shows a destructive interference effect because $r^2 = -t^2$. The probability P_{cd} of seeing photons simultaneously in both beam splitters outputs is zero; the photons always appear as *pairs* in random outputs of the beam splitter.

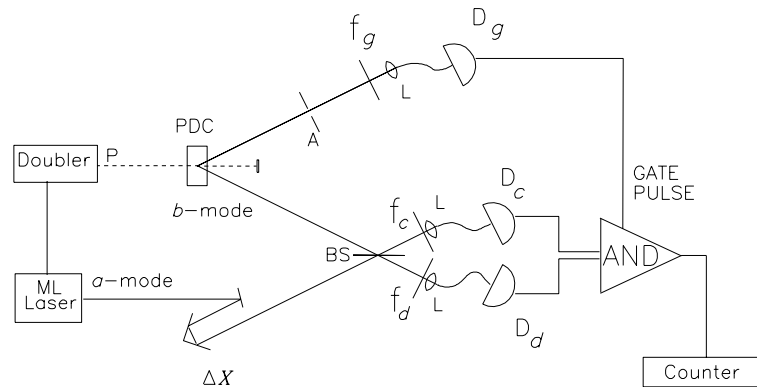Originally, this effect was experimentally demonstrated using the correlated pairs

Figure 4. The experimental apparatus used to demonstrate interference between separate sources. Key: ML, mode locked Ti-Sapphire laser; P, doubled pump beam; PDC, parametric down-conversion crystal; A, aperture; f_g, f_c, f_d, interference filters with 815 nm centre wavelength; L, lenses coupling light to optical fibres; BS, beam splitter; $D_{g,c,d}$, photon counting avalanche photodiodes. Triple coincidences are measured by a gated AND gate. Solid lines indicate light of 815 nm wavelength, dashed lines indicate light of 407.5 nm wavelength and thick curved solid lines represent optical fibres.

of photons produced in the process of parametric down conversion (Hong *et al.* 1987; Rarity & Tapster 1988, 1989). Our interest here is to show that the same interference effect will occur between two single photons which, in principle, could have no common history. This is in preparation for extending the experiment to demonstrate interference and entanglements between arbitrary numbers of separate photons.

We can gate out the one-photon state from a parametric down-conversion source (Rarity *et al.* 1987). The parametric source emits photon pairs simultaneously in correlated directions. Detection of one photon in a particular direction at a particular time is used to locate a single partner photon with an accuracy limited by the detector resolution time which is typically of order 0.4 ns. To overlap two such photons at a beam splitter and make them, in principle, indistinguishable (Rarity 1995), we require an inverse photon bandwidth of order 1 GHz which can be achieved using Fabry–Perot etalons. This leads to low single-photon rates with present parametric down-conversion crystals. Here we choose to time gate using a short (200 fs) pump pulse. The minimum bandwidth associated with a pulse length of a few hundred femtoseconds is then a few nanometres, which is reached by narrow band interference filters.

The experiment is shown in figure 4 (Rarity *et al.* 1997). A frequency-doubled mode-locked laser (407.5 nm wavelength) pumps a thin parametric down-conversion crystal cut for non-degenerate operation. Signal and idler photons satisfying energy conservation are emitted spontaneously in a broad band cone behind the crystal and apertures are placed to select 815 nm wavelength beams from opposite ends of a cone diameter. Detection of an idler (or gate) photon in one beam with time resolution better than the pump pulse separation time essentially localizes a single signal (*b* mode) photon within a pulse length which in the experiment is around 200 fs. The signal photon so selected is a good approximation to a one-photon state and thus must have random phase when we measure it with respect to the original near infrared beam. The two can be thought of as separate sources. Thus, we expect to see no first-order interference fringes when we mix this single-photon source with coherent
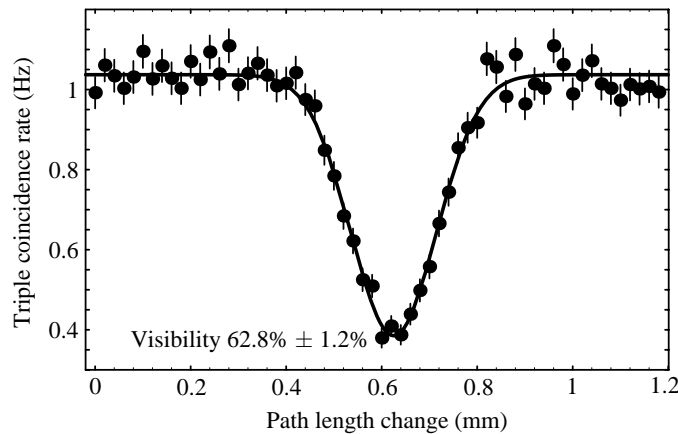
Figure 5. Triple coincidence rate measured as a function of delay ΔX in the weak laser path. Solid line shows a least squares fit based on a Gaussian dip with visibility 64% and 1/e width 133 µm (result reproduced from Rarity *et al.* 1997).

pulses from the undoubled mode-locked laser. However, when we reduce the intensity of the coherent pulses to the point where the energy per pulse is much less than one quantum, we again approximate a one-photon state diluted by a large amount of vacuum. We find that the dominant terms in the state behind a beam splitter are just those highlighted in equation (3.1). When the single photon and coherent pulses overlap, the second-order interference effect leads to a suppression of coincidences after the beam splitter. A typical result showing the gated coincidence rate (triple coincidence) as a function of path length difference altered by an optical trombone in the weak pulse path is shown in figure 5. The interference dip of 63% is beyond the maximum (50%) expected from the second-order interference of two random relative-phase classical pulses.

(b) *Entanglement and non-local interference of two separate sources*

The above experiment can be exended to show a non-local interference effect using the modifications shown in figure 6. Two possible b modes are created at a beam splitter. These different parts of the gated single photon are then mixed at separated beam splitters (BS1 and BS2) with weak coherent pulses of well-defined phases ϕ_1, ϕ_2. The input state to the two beam splitters is now approximated by the product state

$$|\Psi\rangle = \tfrac{1}{2}[(\mathrm{e}^{\mathrm{i}\phi_1}|1\rangle_{a1} + \mathrm{e}^{\mathrm{i}\phi_2}|1\rangle_{a2})(|1\rangle_{b1} + |1\rangle_{b2})], \tag{3.2}$$

where subscripts $a1$, $b1$ define modes propagating to BS1, and $a2$, $b2$ propagating to BS2. In the above approximation we again ignore the large vacuum component of the weak coherent state because we are interested only in coincident pair detection events. Higher-order terms (than $|1\rangle_a$) can be ignored because they are small in the weak coherent state limit (Rarity *et al.* 1997). $|\Psi\rangle$ can be simply expanded to

$$|\Psi\rangle = \tfrac{1}{2}(\mathrm{e}^{\mathrm{i}\phi_1}|1\rangle_{a1}|1\rangle_{b2} + \mathrm{e}^{\mathrm{i}\phi_2}|1\rangle_{a2}|1\rangle_{b1}) + \tfrac{1}{2}(\mathrm{e}^{\mathrm{i}\phi_1}|1\rangle_{a1}|1\rangle_{b1} + \mathrm{e}^{\mathrm{i}\phi_2}|1\rangle_{a2}|1\rangle_{b2}). \tag{3.3}$$

In this last equation the state is separated into two groups of terms. The first set involves one photon at BS1 and the other at BS2, and in the second we see both photons at BS1 OR at BS2. Counting only the coincident detections between the detector set 1 and 2, we elect to study only the first group of terms which are max-
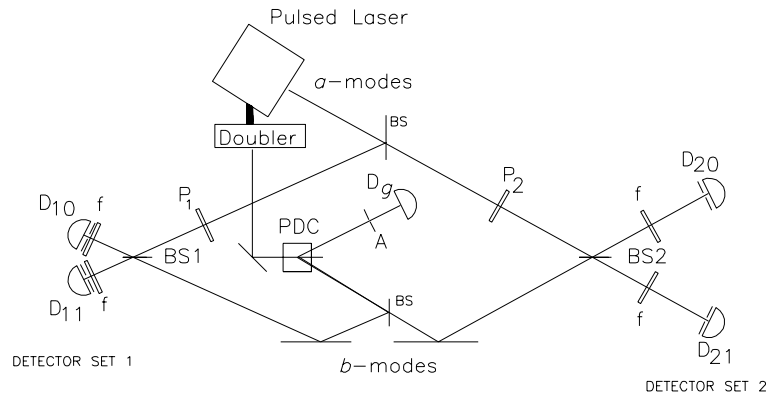
Figure 6. Proposed apparatus to demonstrate a violation of Bell's inequality using heterodyne measurements of a single photon. Key as in figure 4. The *b* mode is split at a beam splitter and recombines with two weak coherent beams (*a* modes) with well-defined phase set by phase shifters P_1 and P_2 at separated beam splitters BS1 and BS2. Measuring triple coincidences between gate *g*, and detector sets 1 and 2 selects an entangled state from the initial product state.

imally entangled. Taken separately, this group of terms can no longer be factorized into a simple (classical) product state.

Using again the beam splitter reflection and transmission coefficients $1/\sqrt{2}$, $i/\sqrt{2}$, the wave function is transformed after BS1 and BS2 to

$$|\Psi\rangle_{bc} = \tfrac{1}{4}[i(e^{i\phi_1} + e^{i\phi_2})|1\rangle_{10}|1\rangle_{20} + i(e^{i\phi_1} + e^{i\phi_2})|1\rangle_{11}|1\rangle_{21}$$
$$+ (e^{i\phi_1} - e^{i\phi_2})|1\rangle_{11}|1\rangle_{20} - (e^{i\phi_1} - e^{i\phi_2})|1\rangle_{10}|1\rangle_{21}]$$
$$+ ie^{i\phi_1}(|2\rangle_{10} + |2\rangle_{11}) + ie^{i\phi_2}(|2\rangle_{20}|0\rangle_{21} + |0\rangle_{20}|2\rangle_{21})]. \tag{3.4}$$

The subcripts 10, 11, 20, 21 now refer to modes after the beam splitters leading directly to similarly labelled detectors (see figure 6). The probability of seeing a coincidence (per pulse) in the 10 and 21 (or the 11 and 20) detectors (gated by a detection in the *g* detector to select out only one-photon states) is

$$P_{12g} = \tfrac{1}{8}C[1 - \cos(\phi_c - \phi_d)], \tag{3.5}$$

where C is the probability of a triple coincidence per pulse in the absence of beam splitters ($C \ll 1$). For coincidences between *c*0, *d*0 or *c*1, *d*1 detectors, the minus is replaced by a plus. The phase adjustments can be performed remote from the sources and we essentially have an apparatus that can be used to demonstrate violations of Bell's inequality (Bell 1964). A similar experiment was first analysed by Tan *et al.* (1989), where the effect was described as a 'Bell inequality of a single photon'. Even when extremely attenuated, the laser can be thought of as a classical field (with a well-defined phase). This experiment can then be thought of as a non-local measurement of the phase of a single photon by heterodyning with a classical field. If we formulate a semiclassical theory where the gated single photon has a definite phase after leaving the crystal, albeit with a randomly varying value from photon to photon, we cannot reproduce the unit visibility interference effect of equation (3.5). The concept of phase of a single photon or in general the phase of a number state is not defined until after measurement.
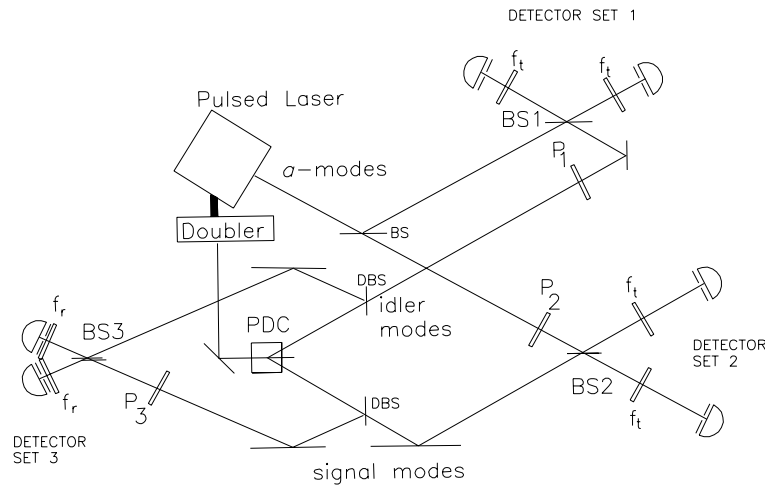
Figure 7. (*a*) Proposed apparatus to demonstrate three-photon interference. We exploit the fact that the phase matching of the down-conversion process allows us to select two pairs of energy matched modes using dichroic beam splitters (DBS) with reflected frequency (f_r) and transmitted frequency (f_t). We now effectively start with an entangled state from the down-conversion crystal which consists of an equal superposition of a reflected signal photon and a transmitted idler OR a transmitted signal and reflected idler photon. We recombine reflected signal and idler modes at beam splitters BS3 and mix the the two transmitted modes with weak coherent states in modes a at beam splitters BS1 and BS2 as shown. Triple coincidence measurements at the beam splitter outputs effectively select out a three-photon entangled state. The distribution of triple coincidences between the eight possible sets of three detectors is altered by altering the phases $\phi_{1,2,3}$ using phase plates $P_{1,2,3}$.

(*c*) *Selecting three particle entanglements using a weak coherent source and pair photon source*

To extend the experiment further we can use both photons from the parametrically generated pair and a weak coherent source to perform a three-photon interference experiment as shown in figure 7. We now label the two down-converted beams as signal s and idler i. Each down-converted beam is split by a dichroic beam splitter into one of two frequencies labelled r (reflected) and t (transmitted). The frequencies f_r and f_t are chosen to satify energy conservation between the two down-converted beams and the pump. As a result, the presence of an idler photon in an r mode is directly correlated with a signal photon in a t mode and vica versa (for example see Rarity & Tapster 1990). The weak coherent beam is split at a standard beam splitter into two a modes which recombine with the transmitted signal and idler modes at two separate beam splitters labelled 1 and 2 (we select only f_t from the weak coherent state using narrowband filters). The reflected signal and idler modes recombine at a third beam splitter BS3. Using the same approximations as in equation (3.2), the state before the remote beam splitters is

$$|\Psi\rangle = \tfrac{1}{2}[(e^{i\phi_1}|1\rangle_{at1} + |1\rangle_{at2})(e^{i(\phi_2+\phi_3)}|1\rangle_{st2}|1\rangle_{ir3} + |1\rangle_{sr3}|1\rangle_{it1})], \qquad (3.6)$$

where subscripts again uniquely label the source (a, s, i), frequency (f_t, f_r) and destination (BS1, 2, 3). When we limit ourselves to three-fold coincidences beyond the beam splitters, we select only

$$|\Psi\rangle = \tfrac{1}{2}[e^{i(\phi_1+\phi_2+\phi_3)}|1\rangle_{at1}|1\rangle_{st2}|1\rangle_{ir3} + |1\rangle_{it1}|1\rangle_{at2}|1\rangle_{sr3}]. \qquad (3.7)$$

This is analagous to the GHZ state introduced by Greenberger *et al.* (1992). The above authors show that for particular settings of the phase triple coincidences will be counted that could not be seen in a comparative classical experiment. This further emphasizes the divergence of quantum mechanics from the classical world view as system size increases.

4. Conclusions

The possibility of building arbitrary superpositions and entanglement of large numbers of initially unconnected one-photon states has been shown. This can be done in theory using an ideal nonlinear element in a Mach–Zehnder interferometer. Such an element is approaching reality in high finesse cavity experiments (Tourchette *et al.* 1995). However, we can go some way to showing higher-order entanglement using linear elements such as beam splitters combined with pair photon sources and weak coherent states. In such experiments we select entangled states from initial product states by measuring three-fold coincident photo-detections. The experiments are limited because the rate of creation of pair photons in parametric down conversion has to remain well below one per coherence time. A further limitation is the effective detector efficiencies seen in these experiments which remain below 20% to date. In the experiments reported here only one triple coincidence per second was counted on average. When we go beyond three- to four-photon experiments with existing apparatus we predict a four-fold coincidence counting rate of around one per hundred seconds.

Within our discussion of quantum gates and quantum computing we have not discussed the problems of decoherence and errors. Such errors can arise from imperfect interference in the interferometers and in the case of the quantum controlled NOT gate from coupling to the environment in the (not so ideal) nonlinear medium. These errors can drastically reduce the performance of any quantum computer of realistic size. However, simple quantum processing such as quantum cryptography is robust even at error rates as high as 1%. These systems are nearing application (Townsend 1997; Zbinden *et al.* 1997*a*,*b*).

References

Barenco, A. 1995 *Proc. R. Soc. Lond.* A **449**, 679–683.

Bell, J. S. 1964 *Physics* **1**, 195.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1992 *J. Cryptology* **5**, 3.

Carnal, O. & Mlynek J. 1991 *Phys. Rev. Lett.* **59**, 2044.

Fearn, H. & Loudon, R. 1987 *Opt. Commun.* **64**, 485–490.

Grangier, P., Roger, G. & Aspect, A. 1986 *Europhys. Lett.* **1**, 173.

Greenberger, D., Horne, M. & Zeilinger, A. 1990 *Am. J. Phys.* **58**, 1.

Hong, C. K., Ou, Z. Y. & Mandel, L. 1987 *Phys. Rev. Lett.* **59**, 2044.

Rarity, J. G. 1995 Fundamental problems in quantum theory. *Ann. NY Acad. Sci.* **755**, 624.

Rarity, J. G. & Tapster, P. R. 1988 In *Photons and quantum flutuations* (ed. E. R. Pike & H. Walther), p. 122. Bristol: Adam Hilger.

Rarity, J. G. & Tapster, P. R. 1989 *J. Opt. Soc. Am.* B **6**, 1221.

Rarity, J. G. & Tapster, P. R. 1990 *Phys. Rev. Letts.* **64**, 2495.

Rarity, J. G., Tapster, P. R. & Jakeman, E. 1987 *Opt. Commun.* **62**, 201.

Rarity, J. G., Tapster, P. R. & Owens, P. C. M. 1994 *J. Modern Opt.* **41**, 2435.

Rarity, J. G., Tapster, P. R. & Loudon, R. 1997 Los Alamos preprint server, quant-ph/9702032.

Shor, P. W. 1994 In *Proc. 35th Annual Symp. on FOCS* (ed. S. Goldwasser), p. 124. Los Alamos, CA: IEEE Computer Society Press.

Tan, S. M., Walls, D. F. & Collett, M. J. 1989 *Phys. Rev. Letts.* **66**, 252–255.

Taylor, G. I. 1909 *Proc. Camb. Phil. Soc.* **15**, 114.

Tourchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. & Kimble, H. J. 1995 *Phys. Rev. Letts.* **75**, 4710.

Townsend, P. D. 1994 *Electron. Lett.* **30**, 809–811.

Townsend, P. D. 1997 *Nature* **385**, 47–49.

Townsend, P. D., Rarity, J. G. & Tapster, P. R. 1993 *Electron. Lett.* **29**, 634.

Zbinden, H., Gautier, J. D., Gisin, N., Muller, A. & Tittel, W. 1997*a* Los Alamos preprint server, quant-ph9703024.

Zbinden, H., Gautier, J. D., Gisin, N., Muller, A. & Tittel, W. 1997*b* *Electron. Lett.* **33**, 586–588.