Linear optical quantum computing and quantum communication gained considerable momentum with the work of Knill, Laflamme and Milburn [6, 7]. They showed that linear optics and projective measurements can efficiently implement quantum computations without the use of Kerr nonlinearities, which are typically very weak. Two key ingredients of linear optical quantum computing (LOQC) are the faithful creation of basic quantum states, such as single-photon states, and the reliable detection of optical output states.

Recently, several groups have demonstrated single-photon sources in quantum-dot microcavities and magneto-optical traps [2, 3, 4]. The importance of these experiments for linear optical quantum computing can hardly be overstated, even though the road to high-visibility interference between independent sources is still long and arduous. Furthermore, Hockney, Dowling and I assessed the quality of single-photon sources by defining the suitability of a source with respect to a given application [5]. In this paper, I turn my attention to the other essential component of LOQC: a photodetector with single-photon resolution.

Most detectors that are currently used in optical quantum communication and computation experiments cannot tell the difference between one or more photons. Single-photon resolution (SPR) detectors are devices that can distinguish between wave packets containing \( n \) and \( n + 1 \) photons [6, 7]. They are important because the LOQC research program relies heavily on projective measurements, which in turn involve photon-number measurements [8, 9]. We therefore need a way to efficiently distinguish between different photon number states. Very often, the output of an optical gate is significantly different when postselected on a single-photon or a two-photon detection outcome. Perhaps the most dramatic example of this is the teleportation experiment by Bouwmeester et al. [10], in which the lack of single-photon resolution reduces the non-postselected fidelity of the teleported output state to a value lower than the classical limit [11, 12]. As a consequence, postselection was needed. Recently, Pan et al. modified the pair-production rates of the two down-converters in this experiment, such that the non-postselected output fidelity surpasses the classical limit [13].

However, it may not always be possible to modify the quantum gate in such a way that non-SPR detectors can be used, and we really would like to have cheap, reliable, and efficient SPR detection devices. But the current experimental detectors with single-photon resolution are expensive and operate at low temperatures [14]. In this paper, I will therefore investigate whether we can build an SPR detector with single-photon sources, linear optics and ordinary photodetection without single-photon resolution. It turns out that such a device is impossible.

Before I proceed with the proof of this statement, I will first simplify the task of the SPR detection device. For many applications it is good enough to distinguish between zero-, one- and two-photon states, rather than the general \( n \)- and \( (n + 1) \)-photon states. Consequently, I will consider only devices that can tell the difference between one- and two-photon states. After all, showing that such a device does not exist immediately excludes the possibility of a general SPR detection device. Also, the SPR device does not have to work with 100% efficiency to be useful (ordinary photodetectors do not, and they are very useful). I will only require that a failure to distinguish between a one- and two-photon input state results in an unambiguous detector signature indicating this failure. This excludes the so-called detector cascade [6, 7], which splits the incoming mode into many outgoing modes to render the probability of finding two photons in the same detector arbitrarily small. However, we can never be certain that two photons didn’t enter the same output mode, and as a consequence, there is no unambiguous detector signature that indicates failure. Here, I will prove that we cannot make an SPR device with a finite number of optical modes that always signals a possible failure unambiguously.

So far, I have been rather vague about the resources that I include for building an SPR device, so I will now...
specify them in more detail. A schematic drawing of the prospective SPR device is shown in Fig. 1 and consists of $M$ input modes, one of which is the mode we want to detect. Without loss of generality, we can choose this to be mode 1. The other modes contain $N-1$ auxiliary photons. So for a single-photon input state, a total of $N$ photons are distributed over $M$ modes according to $\vec{n} = (n_2, \ldots, n_M)$, with $n_i \in \mathbb{N}$ and $\sum n_i = N - 1$.

The $M$ modes are then transformed by a unitary transformation $U$ into $M$ output modes. Every annihilation operator $\hat{a}_i$ corresponding to input mode $a_i$ then becomes a sum of annihilation operators $\hat{b}_k$ that correspond to the output modes $b_k$:

$$\hat{a}_i \rightarrow \sum_{k=1}^{M} U_{ik} \hat{b}_k .$$

Here, we write the transformation in terms of the annihilation operators, but we could also have used the creation operators $\hat{a}_i^\dagger$ and $\hat{b}_k^\dagger$. The commutation relations are the usual:

$$[\hat{a}_i, \hat{a}_j^\dagger] = [\hat{b}_i, \hat{b}_j^\dagger] = \delta_{ij} ,
[\hat{a}_i, \hat{a}_j] = [\hat{b}_i, \hat{b}_j] = [\hat{a}_i^\dagger, \hat{a}_j^\dagger] = [\hat{b}_i^\dagger, \hat{b}_j^\dagger] = 0 ,$$

and all the other commutators vanish. The fact that Eq. 1 does not mix creation and annihilation operators is due to the exclusion of squeezing in the $M$-port $U$.

In principle, we can include feed-forward modes in the transformation $U$. An initial unitary transformation $U_0$ is then followed by a detection of a subset of the outgoing modes. Based on the outcome of this detection, a second unitary transformation $U_1$ is applied to the remaining undetected modes. Again, we detect a subset of the outgoing modes. This procedure repeats itself until all the modes are detected. However, this technique improves only the efficiency, and does not increase the versatility of the device, because for every successful set of detector signatures and unitary transformations $U_0, U_1, \ldots$, we can postpone the intermediate detection events to the very end.

All the outgoing modes are detected with photodetectors that lack single-photon resolution. This amounts to a Projection Operator Valued Measure (POVM) of finding a click $\hat{E}_1$ and finding no click $\hat{E}_0$.

$$\hat{E}_0 = \sum_{n=0}^{\infty} (1 - \eta^2)^n |n\rangle\langle n|$$
$$\hat{E}_1 = \sum_{n=0}^{\infty} [1 - (1 - \eta^2)^n]|n\rangle\langle n| ,$$

where $\eta$ is the quantum efficiency of the detector (that is, every incoming photon triggers the detector with probability $\eta^2$). Since the objective of the proof is to show that SPR detectors cannot be constructed with linear optics and non-photon-resolution detectors, I can choose $\eta \rightarrow 1$. This corresponds to perfectly efficient detectors. If we can’t do it with these, we certainly can’t do it with less sensitive detectors. The POVM thus becomes

$$\hat{E}_0 = |0\rangle\langle 0| \quad \text{and} \quad \hat{E}_1 = \sum_{n=1}^{\infty} |n\rangle\langle n| .$$

The detector signature of the SPR device that should differentiate between one and two input photons is a string $\vec{d} = (d_1, \ldots, d_M)$, where $d_i \in \{ \text{click}, \text{no click} \}$. Any detector signature therefore belongs to one and only one of three sets: the set of signatures that indicate a single photon in the input mode, the set of signatures that indicate two photons, and the set of signatures that indicate a detector failure. This leads to the following criteria:

There are two ways to distinguish one- and two-photon input states: (1) for at least one detector, the output can be a click when one photon enters the device, but does never click when only one photon enters the device; (2) for at least one detector, the output can be a click when two photons enter the device, but does never click when only one photon enters the device. For convenience, let’s call these two methods type I and type II SPR detectors, respectively. I will now prove that it is impossible to distinguish between one- and two-photon input states using either type.

In order to develop a feel for the mechanism of the proof, I will first consider the simplest nontrivial interferometric setup. Suppose that $a_1$ is the input mode that we want to detect, and that there is only a single auxiliary photon in mode $a_2$. The two input modes are transformed according to

$$\hat{a}_1 \rightarrow \alpha \hat{b}_1 + \beta \hat{b}_2 \quad \text{and} \quad \hat{a}_2 \rightarrow \gamma \hat{b}_1 + \delta \hat{b}_2 .$$

A single-photon input with one auxiliary photon then yields the polynomial

$$\hat{a}_1 \hat{a}_2 \rightarrow \alpha \gamma \hat{b}_1^2 + (\alpha \delta + \beta \gamma) \hat{b}_1 \hat{b}_2 + \beta \delta \hat{b}_2^2 ,$$

whereas two input photons yield

$$\hat{a}_1^2 \hat{a}_2 \rightarrow \alpha^2 \gamma \hat{b}_1^3 + (2\alpha \beta \gamma + \alpha^2 \delta) \hat{b}_1^2 \hat{b}_2 + (2\alpha \beta \delta + \beta^2 \gamma) \hat{b}_1 \hat{b}_2^2 + \beta^2 \delta \hat{b}_2^3 .$$

FIG. 1: The general setup for the single-photon resolution detection device with linear optics and projective measurements. The aim of this detector is to distinguish between one and two photons in the input mode. The auxiliary modes are occupied by photon-number states, and the detectors click only when one or more photons are present.
If the detection device is not to fire at a two-photon input, all the terms involving $\hat{b}_1$ must have zero coefficients (we can choose $\hat{b}_1$ without loss of generality). We start with the leading term $\hat{b}_1^3$.

For the polynomial in Eq. (7) to have no $\hat{b}_1^3$ contribution, we need to put $\alpha^2 \gamma = 0$, which implies either $\alpha = 0$ or $\gamma = 0$. Secondly, we require that $2\alpha \beta \delta + \beta^2 \gamma = 0$. If $\alpha$ and $\gamma$ are not zero simultaneously, we also arrive at the conclusion that $\beta = 0$ or $\delta = 0$. With these restrictions, it is no longer possible to choose $(\alpha, \beta, \gamma, \delta)$ such that the single-photon input of Eq. (6) retains a non-zero contribution, we need to put $\alpha = 0$ or $\gamma = 0$, which implies either $\alpha = 0$ or $\gamma = 0$. Since this holds true for all $l$, we only have to consider the case where $\exists q : \alpha_q = 0$, or $\forall l : \alpha_{pl} = 0$. After all, if only some $\alpha_{pl}$ are zero, there must be a $\alpha_q = 0$, and there is therefore no need for $\alpha_{q} = 0$. However, setting all $\alpha_{q} = 0$ is equivalent to removing the $p^{th}$ input photon. Since we set this proof up for an arbitrary number of auxiliary photons, we only have to consider $\alpha_{q} = 0$.

The next term in Eq. (7) the coefficient of which has $\alpha_{l1} \cdots \alpha_{N1} = 0$ (12).

If $\alpha_{p1} = 0$, then only one term remains:

$$\alpha_{11} \cdots \alpha_{pl} \cdots \alpha_{N1} = 0$$

(13)

and this forces a second matrix element $\alpha_{q1}$ or $\alpha_{pl}$ to zero. Since this holds true for all $l$, we only have to consider the case where $\exists q : \alpha_{q1} = 0$, or $\forall l : \alpha_{pl} = 0$. After all, if only some $\alpha_{pl}$ are zero, there must be a $\alpha_{q1} = 0$, and there is therefore no need for $\alpha_{q} = 0$. However, setting all $\alpha_{q} = 0$ is equivalent to removing the $p^{th}$ input photon. Since we set this proof up for an arbitrary number of auxiliary photons, we only have to consider $\alpha_{q1} = 0$.

The next term in Eq. (7) the coefficient of which has to be zero, is $\hat{b}_1^{N-1} \hat{b}_1 \hat{b}_1$. With $\alpha_{p1} = 0$ and $\alpha_{q1} = 0$, the remaining term is

$$\alpha_{11} \cdots \alpha_{pn} \cdots \alpha_{qn} \cdots \alpha_{N1} = 0$$

(14)

and this leads to the conclusion that there must be an $\alpha_{r1} = 0$.

We can repeat this process such that for each $k$ in the terms involving $\hat{b}_k^l$, we find an $\alpha_{r1} = 0$. There are $N + 1$ terms with an overall factor $\hat{b}_k^l$, but there are only $N$ terms $\alpha_{r1}$. We thus have forced all $\alpha_{r1}$ to zero, and the single-photon input will also have a zero amplitude in mode $\hat{b}_1$:

$$\hat{a}_1 \prod_{m=2}^N \hat{a}_m \to \prod_{m=1}^N \left( \sum_{j=1}^M \alpha_{mj} \hat{b}_j \right)_{|\alpha_{m1}=0} \right)$$

(15)

Since I explicitly constructed the SPR detection device to signal the presence of a single photon in mode $\hat{b}_1$, Eq. (15) contradicts the premise. Hence, an SPR detector of type I is impossible.

Secondly, I consider the type II SPR detector, that is, for at least one detector, the output is a click when two photons enter the device, and no click when only one photon enters the device. The impossibility proof runs along the same lines as the previous proof. With a single photon in the input mode, the output before the detectors is then

$$\hat{a}_1 \prod_{m=2}^N \hat{a}_m \to \prod_{m=1}^N \left( \sum_{j=1}^M \alpha_{mj} \hat{b}_j \right)_{|\alpha_{m1}=0} \right)$$

(16)
Here, I have already used the fact that all $N-1$ auxiliary photons should be distributed over different modes. Following the same line of reasoning, all the $N$ matrix elements $\alpha_{r1}$ with $r \in \{1, \ldots, N\}$ are forced to zero by the $N$ different $k$-terms proportional to $\hat{b}_k^\dagger$. Again, this excludes the possibility for two input photons to trigger the detector in output mode 1. Therefore, an SPR detector of type II is impossible as well, which means that single-photon–resolution detection devices with auxiliary photon-number input states, linear optics and projective measurements are impossible.

As I mentioned before, a detector cascade can succeed with arbitrary large probability of success where the above SPR device fails. Braunstein and I have shown in Ref. [6] that such cascades need a large number of output modes, and that they are very sensitive to detector losses. Notwithstanding these difficulties, Haderka et al. have made significant experimental progress towards a working detector cascade. Nevertheless, I believe this theorem is an interesting property of linear optics with the projective measurements I presented here, and it might be useful in guiding our intuition when we try to develop interferometers that are to perform special tasks in linear optical quantum computing and communication.

This work was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. I would like to thank Bill Munro for stimulating discussions and valuable comments, and Jonathan Dowling for carefully reading this manuscript. I also acknowledge the United States National Research Council. Part of this research was carried out in the Centre for Quantum Computer Technology at the University of Queensland, Australia.

[1] E. Knill, R. Laflamme, and G.J. Milburn, Nature (London) 409, 46 (2001).
[2] C. Santori, D. Fattal, J. Vučić, G. S. Solomon, and Y. Yamamoto, Nature (London) 419, 594 (2002).
[3] A. Kuhn, M. Hennrich, and G. Rempe, Phys. Rev. Lett. 89, 067901 (2002).
[4] M. Pelton, C. Santori, J. Vučić, B. Zhang, G.S. Solomon, J. Plant, and Y. Yamamoto, Phys. Rev. Lett. 89, 233602 (2002).
[5] G.M. Hockney, P. Kok, and J.P. Dowling, Phys. Rev. A 67, 0323XX (2003).
[6] P. Kok and S.L. Braunstein, Phys. Rev. A 63, 033812 (2001).
[7] O. Haderka, M. Hamar, and J. Perina Jr., Experimental multi-photon-resolving detector using a single avalanche photodiode, quant-ph/0302154; J. Reháček, Z. Hradil, O. Haderka, J. Perina Jr., and M. Hamar, Multiple-photon resolving fiber-loop detector, quant-ph/0303032.
[8] H. Lee, P. Kok, N.J. Cerf, and J.P. Dowling, Phys. Rev. A 65, 030101 (2002).
[9] P. Kok, H. Lee, and J.P. Dowling, Phys. Rev. A 66, 063814 (2002).
[10] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) 390, 575 (1997).
[11] S.L. Braunstein and H.J. Kimble, Nature (London) 394, 840 (1998).
[12] P. Kok and S.L. Braunstein, Phys. Rev. A 61, 042304 (2000).
[13] J.-W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, Nature (London) 421, 721 (2003).
[14] S. Takeuchi, J. Kim, Y. Yamamoto, and H.H. Hogue, Appl. Phys. Lett. 74, 1063 (1999); J. Kim, S. Takeuchi, Y. Yamamoto, and H.H. Hogue, ibid. 74, 902 (1999); A.J. Miller, S.W. Nam, and J.M. Martinis, Demonstration of a broadband photon-number resolving detector, privately communicated document, 25 October, 2002.
[15] P. Kok and S.L. Braunstein, Phys. Rev. A 62, 064301 (2000).