Quantum error correction for communication with linear optics

Samuel L. Braunstein

SEECS, University of Wales, Bangor LL57 1UT, UK

Improving the signal-to-noise ratio in optical communication systems is a fundamental requirement for cost-effective data transmission. This is particularly important for the transmission of noise-intolerant quantum states: excess noise at the quantum level destroys the coherence of the states, rendering classical error correction or amplifier-based schemes[1] useless for quantum communication. Only quantum error correction[2,3] can remove the effects of noise without corrupting the fragile superpositions of quantum states. But difficulties arise in the practical implementation of such a correction process because nonlinear operations[4] have been thought to be required, greatly reducing the efficiency of any optical scheme. Here I report an efficient, compact scheme involving only linear optical elements and feedback, which performs error correction for both quantum and classical noise. In the classical case, the noise penalty incurred is no worse than for ideal amplification. But for low-noise quantum optical communication, this penalty may be eliminated entirely. This quantum error-correction scheme may thus find application in quantum cryptographic networks[5–7] (where low noise is equivalent to high security), possibly extending their range far beyond limits imposed by system losses[7].

The discovery of quantum error-correcting codes[2,3] substantially enhanced the feasibility of building a quantum computer and of one day using it to efficiently factor large numbers[8]. The basis of this substantial advance lies in the ability to tame the hazards of decoherence by encoding the information of a given state in a set of entangled states, without violating the no-cloning theorem of quantum mechanics[9]. Recently, quantum error-correction protocols have been extended from discrete quantum variables, such as quantum bits (qubits), to continuous ones, such as arbitrary-intensity optical wavepackets[10,11]. Implementing continuous quantum error correction in optical communications systems is, therefore, the next logical step. Yet, the prevailing view had been that nonlinear operations, such as the exclusive-OR gate[4], are essential for a compact construction. According to this view, replacing these nonlinear components by linear ones would require an exponential increase in their number[12]. A hint that we may be able to use only a handful of linear optical elements when dealing with continuous variables is found in a recent realization[13] of quantum teleportation using only beam-splitters, feedback and a source of optical squeezed states[14]. The degree of squeezing would determine the noise penalty in the correction fidelity: completely classical light would cause relatively small, finite errors, and perfect squeezing would yield an ideal quantum optical repeater.

The implementation I describe here involves a nine-wavepacket code, which completely encodes the full quantum state of a single wavepacket such that if one of those nine wavepackets were to be disturbed in any way the original information may be recovered[10,11]. This nine-wavepacket code is the continuous-variable analogue of Shor's original code for discrete quantum states[2]. To implement Shor's qubit code using only linear operations would require $2^9 = 512$ channels and exponentially many more components[12]. By contrast, the code described here uses nine channels and encoding is performed with only eight beam-splitters. An optimal-efficiency five-wavepacket code (with the same encoding and noise-resistant properties) has recently been found[10]. I prefer to work with the nine-wavepacket code here, owing to its simple and intuitive structural properties.

I focus attention on the state of a single polarization of a transverse mode of electromagnetic radiation, which may be succinctly described by a one-dimensional wavepacket. As the electric quadrature amplitudes (the real and imaginary parts of the complex electric field) form a canonically conjugate pair, in analogy with position and momentum, it is convenient to use the latter terms. In a units-free notation:

$$\text{position} = xL$$

$$\text{momentum} = p/L \qquad (1)$$

where x and p are scaled position and momentum (with some arbitrary length scale L) and $\hbar = 1/2$. (I henceforth drop the modifier 'scaled'.) The position basis eigenstates $|x\rangle$ are normalized according to $\langle x'|x\rangle = \delta(x' - x)$ with the momentum basis given by:

$$|p\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} \mathrm{d}x e^{2ixp} |x\rangle \qquad (2)$$

To avoid confusion, I shall work in the position basis throughout. The Fourier transform is defined as an active operation on a state by

$$\hat{F}|x\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} \mathrm{d}y e^{2ixy} |y\rangle \qquad (3)$$

where both x and y are variables in the position basis and symbols marked with a circumflex denote linear operators. Note that equations (2) and (3) correspond to a change of representation and a physical change of state, respectively. For optical wavepackets this Fourier transform describes the action of a 1/4-wave delay.

It turns out that all one needs to construct an encoding element is a series of beam-splitters and phase delays. The linearity of the coding device is facilitated by the freedom in the choice of length scale in equation (1), which is meaningful only for systems with continuous variables.

I now seek a device that will encode a position-state eigenstate $|x\rangle$ in a nine-wavepacket code of the form[10]:

$$|x_{\text{encode}}\rangle = \frac{1}{\pi^{3/2}} \int \mathrm{d}w \mathrm{d}y \mathrm{d}z e^{2ix(w+y+z)} \times |w, w, w, y, y, y, z, z, z\rangle \qquad (4)$$

First, consider two light fields $|x\rangle$ and $|y\rangle$ incident on an 'ideal' (phase-free) beam-splitter. The output light fields are given by:

$$\hat{B}_{12}(\theta)|x, y\rangle = |x\cos\theta - y\sin\theta, y\cos\theta + x\sin\theta\rangle \qquad (5)$$

where the subscripts 12 refer to the wavepackets acted upon. From these ideal beam-splitters I construct a three-port device called a tritter[15]:

$$\hat{T}_{123} \equiv \hat{B}_{23}(\pi/4)\hat{B}_{12}\left(\cos^{-1}\frac{1}{\sqrt{3}}\right) \qquad (6)$$

for which $\hat{T}_{123}|x, 0, 0\rangle = |x/\sqrt{3}, x/\sqrt{3}, x/\sqrt{3}\rangle$. Finally, all the above elements are combined to produce the encoding device. A suitable choice for the nine-wavepacket code is a nine-port beam-splitter, which I shall call a nona-splitter:

$$\hat{N}_{1-9} \equiv \hat{T}_{789}\hat{T}_{456}\hat{T}_{123}\hat{F}_7\hat{F}_4\hat{F}_1\hat{T}_{147} \qquad (7)$$

where I have not explicitly included the free propagation factors between optical elements. This device could be implemented either as a series of eight ordinary beam-splitters or as a single (mass-produced) integrated-optics element.

The nine-wavepacket code, equation (4), may now be formed with the nona-splitter acting on the initial unencoded state, via $|x_{\text{encode}}\rangle \propto \hat{N}_{1-9}|x_{\text{init}}\rangle$. Written in this order, $\hat{F}_7\hat{F}_4\hat{F}_1\hat{T}_{147}$ forms the momentum-error-correction code (or Fourier-transformed position code), and the remaining tritters $\hat{T}_{789}\hat{T}_{456}\hat{T}_{123}$ form the position-error-correction codes for each of the three momentum-encoded wavepackets.

By linearity, it is sufficient to consider the encoding procedure on

a position eigenstate $|x\rangle$. The eight auxiliary inputs are prepared with zero-position eigenstates (that is, ideally squeezed states, an assumption that is relaxed below), so the initial unencoded state has the form $|x_{\text{init}}\rangle = |x, 0, 0, 0, 0, 0, 0, 0, 0\rangle$. Having introduced the coding device, I proceed with a discussion of the error detection and correction procedure. The three states constituting error correction described here are: inverted encoding, error-syndrome identification and error correction. In the case of perfect signal-transmission, inverted encoding trivially recovers the initial (unencoded) state with the auxiliary wavepackets returning to their zero positions. If, however, one of the encoded wavepackets suffers from noise, then following inverted encoding the auxiliary wavepackets will display a non-zero 'syndrome', indicating the type and size of the error. More specifically, position measurements are performed on each of the eight auxiliary ports. Syndrome identification then involves only simple comparisons between these real numbers. Once identified, the syndrome is translated to the appropriate remedy which, for my scheme, corresponds to a pure linear displacement (whose parameters are obtained by a linear combination of these real numbers). This remarkable fact, that an arbitrary error can be corrected with a linear displacement, is general and very important for purposes of implementation.

As an example, consider an inverted encoding algorithm which inverts $\hat{N}_{1-9}$ in two steps, enabling independent correction of position and momentum errors. First I invert the last three tritters (those to the left) in equation (7) and identify the syndrome for the position error. There are three sets of syndromes here corresponding to the positions of auxiliary wavepackets (2, 3), (5, 6) and (8, 9). Then I invert the remaining terms to obtain the momentum error. The syndrome in this case is given by the positions of auxiliary wavepackets 4 and 7. Finally, I perform a linear displacement based on the identified syndrome and retrieve the original wavepacket.

So far, I have presented the error-correction code and procedure. This code will operate ideally (that is, perform perfect error-correction) under noise-free conditions, corresponding to ideal-squeezing of the auxiliary wavepackets, noiseless manipulation and perfect detection. (Indeed, this is also the prediction one would obtain from classical wave theory.) What would be the penalty of operating this scheme with imperfect resources and detection? As a first source of errors, I examine the use of auxiliary wavepackets with an initial squeezing parameter r and uncertainty $e^{-r}/2$. Moreover, I suppose that the position measurements necessary for reading the error-syndrome are carried out by homodyne detectors with an energy efficiency η, yielding a noise term that is represented by vacuum leakage (with uncertainty 1/2) into the device[13]. In this case, the jth component of the syndrome x_{syn} (that is, the position measured at the jth output port) becomes randomized by the uncertainty. Thus, for an error originating on the kth wavepacket ($k = 1 \ldots 9$) each component of the syndrome takes the generic form:

$$x^j_{\text{syn}} = x^j_{0,\text{syn}} + \sum_l c^k_{jl} x^l_{\text{sq}} + \sqrt{\eta^{-1} - 1}\, x'^j_{\text{vac}} \qquad (8)$$

Here $x_{0,\text{syn}}$ is the ideal syndrome, and x_{sq} and x'_{vac} are noise terms due to limited squeezing of the input states and imperfect detection at the output, respectively, for some constants c^k_{jl}.

Under these noisy conditions, some non-zero syndrome will always be identified, even in the absence of an actual error (to the encoded state). Correcting fictitious errors accumulates small yet undesired penalties. A more careful, bayesian, approach to syndrome identification may avoid this and would be especially useful when real errors occur rarely per error-correction cycle. Precisely how big would the penalty be if correction was carried through? After displacement, the output state may be represented as a Wigner function by a convolution of the Wigner function of the original unencoded state with an error gaussian $\exp[-2|\alpha|^2/(e^{-2r} + \eta^{-1} - 1)]$ (up to normalization). For the case of efficient detection but auxiliary wavepackets in the vacuum state, this gaussian reduces to the Wigner representation for vacuum, and a noise penalty of roughly one unit of vacuum fluctuations is incurred[16]. By squeezing the auxiliary wavepackets, even this penalty may be reduced to allow for long-distance, error-corrected quantum state transmission.

Perhaps the most promising potential application of quantum error correction within an optical channel lies in quantum cryptography. Today, system losses impose a limit to the range of quantum communication[7]. Quantum error correction can be applied to attack this problem, both in the case of the cryptographic transmission of continuous variables and in more conventional qubit-transmission. In the former case, this calls for further consideration of recently proposed schemes for ideal (noiseless) continuous-variable quantum cryptography[17,18]. For finite squeezing or imperfect detection, however, some residual noise will be present. This noise has the effect of helping the eavesdropper mask her attack, so our guarantee of absolute security is lost.

The ability to encode qubits in continuous variables suggests a more likely alternative for implementation within my quantum error-correction scheme. There are several ways qubits could be represented within our scheme. They could be encoded as polarizations (requiring a duplication of our scheme for each polarization channel)[5]. Less expensive alternatives might involve encoding qubits as the phase between pulses in unbalanced Mach–Zehnder interferometers[6], or encoding them as the time between pulses in interferometers using Faraday mirrors[7]. All of these schemes have been implemented in quantum cryptography. Unlike continuous variable schemes, there exist well-developed methods for dealing with noise in qubit-based quantum cryptography including classical[19] and quantum[20] privacy amplification.

Finally, I consider the performance of my error-correction scheme as a classical tool for long-distance communication and data-transmission. In particular, can error correction provide a realistic alternative to amplifier-based repeaters? First, I note that amplifier-based repeaters are phase insensitive, while for error-correction a high degree of interferometric stability is required. Having said this, the low noise in my scheme still offers possible advantages over conventional amplification methods. Even though the basic penalty of one unit of vacuum fluctuations for my scheme is equal to that of strongly amplifying a signal with an ideal amplifier[1], distributing amplifiers along a channel introduces extra complications: an amplifier placed at the beginning of a channel produces a greater energy throughput, thus requiring higher channel capacities. By comparison, in error-correction schemes, a fixed reduction of channel capacity is incurred due to the transmission of redundant information in the auxiliary wavepackets. This penalty can, in principle, be made arbitrarily small for asymptotically efficient codes. Amplifiers also suffer penalties when placed at the end of channels, as the additional noise from the channel is amplified along with the signal. By contrast, my scheme is designed to correct errors, rather than maintain the signal-to-noise ratio. One example of a difficulty faced by conventional amplification schemes is the occurrence of large burst errors in space communications. Using only classical resources (that is, $r = 0$), my scheme would correct single wavepacket errors independent of the burst intensity.

Quantum error correction will almost certainly play an important role in new technologies based on quantum information. I have shown that continuous error correction can be achieved in an interferometric set-up with only a handful of linear components and a standard quantum resource: squeezed states of light. By comparison, standard quantum computational networks acting on discrete states require similar numbers of nonlinear components. Maintaining the interferometric stability required for operating the proposed scheme would appear to be feasible with today's technology. Moreover, I have shown that even in the absence of

squeezing, the scheme's performance is remarkably good, closely competing with ideal amplifier-based repeaters. Replacing such repeaters may become the first implementation of quantum-computational concepts to (real-world) classical problems. □

Received 8 December 1997; accepted 14 April 1998.

1. Haus, H. A. & Mullen, J. A. Quantum noise in linear amplifiers. *Phys. Rev.* **128,** 2407–2413 (1962).
2. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52,** R2493–R2496 (1995).
3. Steane, A. M. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77,** 793–797 (1996).
4. DiVincenzo, D. P. & Smolin, J. in *Proc. Workshop on Physics and Computation PhysComp '94* 14–23 (IEEE Computer Soc. Press, Los Alamitos, CA, 1994).
5. Bennett, C. H. & Brassard, G. The dawn of a new era for quantum cryptography: the experimental prototype is working! *SIGACT News* **20,** 78–82 (1989).
6. Townsend, P. D., Rarity, J. G. & Tapster, P. R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel. *Electron. Lett.* **29,** 1291–1293 (1993).
7. Muller, A. *et al.* Plug and play systems for quantum cryptography. *Appl. Phys. Lett.* **70,** 793–795 (1997).
8. Shor, P. W. in *Proc. 35th Annual Symp. on the Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Soc. Press, Los Alamitos, CA, 1994).
9. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
10. Braunstein, S. L. Error correction for continuous quantum variables. *Phys. Rev. Lett.* **80,** 4084–4087 (1998).
11. Lloyd, S. & Slotine, J.-J. E. Analog quantum error correction. *Phys. Rev. Lett.* **80,** 4088–4091 (1998).
12. Reck, M. *et al.* Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73,** 58–61 (1994).
13. Braunstein, S. L. & Kimble, H. J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **80,** 869–872 (1998).
14. Walls, D. F. Squeezed states of light. *Nature* **306,** 141–146 (1983).
15. Zukowski, M. Entanglement and photons. *Laser Phys.* **4,** 690–709 (1994).
16. Musslimani, Z. H., Braunstein, S. L., Mann, A. & Revzen, M. Destruction of photocount oscillations by thermal noise. *Phys. Rev. A* **51,** 4967–4973 (1995).
17. Mu, Y., Seberry, J. & Zheng, Y. Shared cryptographic bits via quantized quadrature phase amplitudes of light. *Opt. Commun.* **123,** 344–352 (1996).
18. Cohen, O. Quantum cryptography using nonlocal measurements. *Helv. Phys. Acta* **70,** 710–726 (1997).
19. Bennett, C. H., Brassard, G. & Robert, J.-M. Privacy amplification by public discussion. *SIAM J. Comput.* **17,** 210–229 (1988).
20. Deutsch, D. *et al.* Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77,** 2818–2821 (1996).

Acknowledgements. I thank N. Cohen, H. J. Kimble and A. M. Steane for discussions.

Correspondence and requests for materials should be addressed to the author (e-mail: schmuel@sees.bangor.ac.uk).

Nanofabrication of solid-state Fresnel lenses for electron optics

Y. Ito, A. L. Bleloch & L. M. Brown

Department of Physics, University of Cambridge, Cavendish Laboratory, Madingley Road, Cambridge CB3 0HE, UK

Lenses for precision electron optics are mainly magnetic, requiring large cylinders of soft iron to focus an electron beam. Such lenses can only be convergent[1], and so suffer from spherical aberration. Electrostatic lenses are sometimes used, but tend to be even more cumbersome. The advent of high-brightness electron guns for scanning transmission electron microscopy has made it possible to use the resulting tightly focused electron beams to drill holes a few nanometres in size and of controlled depth in some inorganic thin films[2–5]: such patterned structures can then be used to manipulate the phase of an electron wave in a manner analogous to light optics[6,7]. Here we use this approach to fabricate compact solid-state 'pixelated' Fresnel lenses for electron optics. These lenses, which can be convergent or divergent, are not expected to compete with conventional magnetic lenses in most applications (such as microscopy), but may find a niche in electron-beam lithography.

In order to focus an incident electron plane wave (wavelength λ), it must undergo a phase retardation $\phi(r)$ which varies with the radius from the optic axis, r, as follows:

$$\phi(r) = k_0(f - (f^2 + r^2)^{1/2}) \quad (1)$$

where $k_0 = 2\pi/\lambda$ and f is the focal length of the lens[8].

$\phi(r)$ can be modified to have a modulo 2π phase structure, and the phase distribution of a zone, $\phi_F(r)$, becomes:

$$\phi_F(r) = \phi(r) + 2m\pi, \qquad r_m < r < r_{m+1} \quad (2)$$

where r_m is the inner radius of the mth zone. Equation (2) can, of course, be modified to include any additional phase to correct

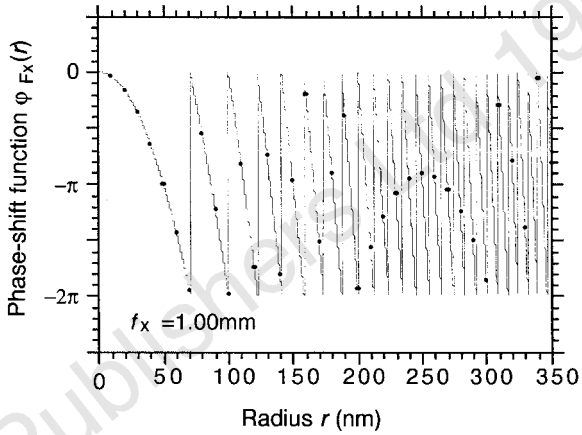

Figure 1 Phase-shift function, $\phi_F(r)$, of the ideal Fresnel lens (line) and the radial positions of the holes and their expected phase shifts for the actual lens (dots) with a nominal focal length of $f = 1$ mm. Because the dwell time of the beam for each hole is controlled, the expected phase values were calculated from the linear relationship between the dwell time and the desired phase here. For the higher-order zones, an aliasing effect between the hole position and $\phi_F(r)$ can be seen. The minimum zone width is limited by the size of a single hole (~2 nm).

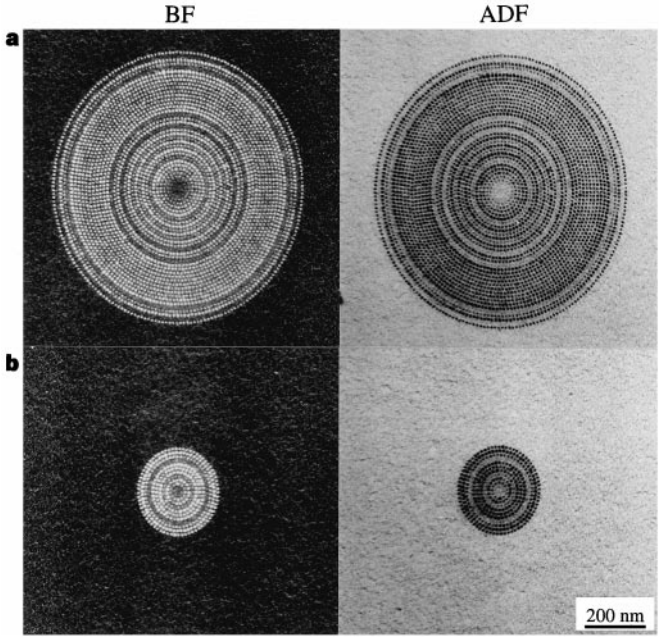

Figure 2 Two Fresnel lenses with different focal lengths. Bright field (BF) and high angle annular dark field (ADF) images of nominal focal length of **a**, $f = 1$ mm and **b**, $f = 0.25$ mm lenses. The diameters of each lens are **a**, 700 nm and **b**, 236 nm. Before observation, the lenses were fabricated in VG HB501 STEM with a probe current of ~200 pA at 100 keV. An a-AlF_3 film, 68 nm thick, was overwritten 30 times with the lens pattern. The total fabrication time for the lenses was 60 s and 6 s for **a** and **b**, respectively. A single zone has the same width as the hole spacing from the 10th ($r_m = 316$ nm) and 3rd ($r_m = 112$ nm) zone outwards for **a** and **b**, respectively. The outer zones beyond half of the radius demonstrate this aliasing effect.