



MIT Open Access Articles

Reading boundless error-free bits using a single photon

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation	Guha, Saikat, and Jeffrey H. Shapiro. "Reading boundless error-free bits using a single photon." <i>Physical Review A</i> 87, no. 6 (June 2013). © 2013 American Physical Society
As Published	http://dx.doi.org/10.1103/PhysRevA.87.062306
Publisher	American Physical Society
Version	Final published version
Citable link	http://hdl.handle.net/1721.1/80298
Terms of Use	Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.

Reading boundless error-free bits using a single photon

Saikat Guha¹ and Jeffrey H. Shapiro²

¹*Quantum Information Processing (QuIP) Group, Raytheon BBN Technologies, Cambridge, Massachusetts 02138, USA*

²*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 26 July 2012; revised manuscript received 15 February 2013; published 6 June 2013)

We address the problem of how efficiently information can be encoded into and read out reliably from a passive reflective surface that encodes classical data by modulating the amplitude and phase of incident light. We show that nature imposes no fundamental upper limit to the number of bits that can be read per expended probe photon and demonstrate the quantum-information-theoretic trade-offs between the photon efficiency (bits per photon) and the encoding efficiency (bits per pixel) of optical reading. We show that with a coherent-state (ideal laser) source, an *on-off* (amplitude-modulation) pixel encoding, and shot-noise-limited direct detection (an overly optimistic model for commercial CD and DVD drives), the highest photon efficiency achievable in principle is about 0.5 bits read per transmitted photon. We then show that a coherent-state probe can read unlimited bits per photon when the receiver is allowed to make joint (inseparable) measurements on the reflected light from a large block of phase-modulated memory pixels. Finally, we show an example of a spatially entangled nonclassical light probe and a receiver design—constructible using a single-photon source, beam splitters, and single-photon detectors—that can in principle read any number of *error-free* bits of information. The probe is a single photon prepared in a uniform coherent superposition of multiple orthogonal spatial modes, i.e., a W state. The code and joint-detection receiver complexity required by a coherent-state transmitter to achieve comparable photon efficiency performance is shown to be *much* higher in comparison to that required by the W -state transceiver, although this advantage rapidly disappears with increasing loss in the system.

DOI: [10.1103/PhysRevA.87.062306](https://doi.org/10.1103/PhysRevA.87.062306)

PACS number(s): 42.50.Ex, 03.67.Hk, 42.79.Sz, 42.30.Lr

I. INTRODUCTION

Optical discs, such as compact discs (CDs) and digital video discs (DVDs), are ubiquitous. The surface of the CD contains a long spiral track of data, along which there are flat reflective areas called *land* and nonreflective *bumps* (see Fig. 1), representing binary 1 and binary 0, respectively. The drive shines a laser at the surface of the CD to read data. The detector photocurrent tracks the intensity of the reflected light, which the drive converts into estimates of 1s and 0s. There is an extensive literature and ongoing research on evaluation of information-theoretic capacities of optical storage, error-correcting codes, and techniques to make the storage and readout more efficient [1,2]. The majority of that work, however, concentrates on what can be achieved by optimizing existing technology, as opposed to establishing what are the true ultimate limits—imposed by the laws of quantum mechanics—on optical reading of information that has been encoded into a passive reflecting medium.

Fundamentally, the performance of any optical communication or imaging system is limited by noise of quantum-mechanical origin, and optical reading of information is no exception. In order to delineate the ultimate performance of optical reading limited only by the laws of physics, an analysis within a full quantum-mechanical framework must therefore be done. Some examples of early work relevant to quantum reading include Shapiro's *number-product vacuum* states for zero-error reading of phase-conjugate-encoded pixels [3], Acin's work on optimally distinguishing two unitary transformations [4], and D'Ariano *et al.*'s demonstration that entanglement can improve the precision of estimating an unknown transformation [5]. In a suite of recent work by Pirandola and others [6–13], it has been shown that nonclassical light paired with nonstandard detection techniques

can read data more reliably than can a coherent-state (laser) probe; i.e., at a given transmitted-photon budget the former can discriminate between a set of reflectivity-phase values for a pixel with a lower probability of error than the latter.

Lower error probability in discriminating signals from a modulation constellation does not automatically translate to increased *capacity*, i.e., the sustained reliable rate of reading that is achievable with an optimal modulation, code, and receiver. Attaining the quantum-limited capacity—the *Holevo limit* [14,15]—requires joint-detection receivers (JDRs), whenever the modulation constellation's quantum states are not mutually orthogonal. JDRs make collective measurements on the reflected light from many memory pixels—which cannot be realized by detecting the reflected light from each pixel individually—followed by optimal joint postprocessing of the classical measurement outcomes [16]. Recent work on the capacity of optical reading [7] evaluated achievable rates that employ JDRs to detect code words constructed from binary-amplitude pixel modulation. These achievable rates, however, fall significantly short—in both the capacity and photon efficiency of optical reading—when amplitude *and* phase modulation are taken into account.

In this paper, we address the following fundamental question: What is the ultimate upper limit to the number of bits of information that can be reliably read using an optical probe with a given mean photon-number budget when information is encoded using a reflective surface that can passively modulate a combination of the amplitude and phase of the probe light [17]? We show that there is no upper limit to the number of bits that can be read reliably per expended photon. We also show that with a coherent-state source, an on-off pixel modulation, and ideal direct detection (an overly optimistic model for commercial CD and DVD drives), the highest photon

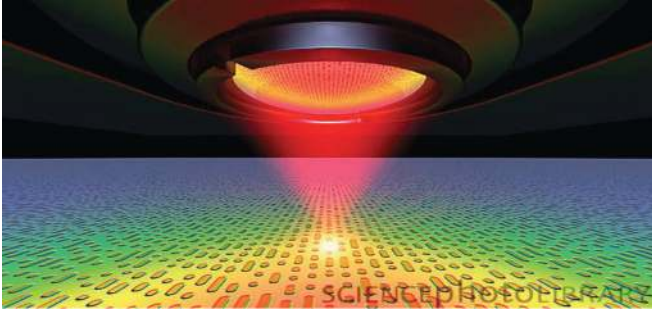


FIG. 1. (Color online) Artist's impression of the CD drive's read laser shining on the surface of an optical disk (picture courtesy of Science Photo Library).

information efficiency (PIE) achievable is about 0.5 bits per transmitted photon. We then show that a coherent-state probe can read boundless bits per transmitted photon when the receiver is allowed to make joint measurements on the reflected light from a large block of phase-modulated memory pixels. We show one structured design for such a JDR that can attain an unbounded PIE with a coherent-state transmitter, which is not possible using any conventional optical transceiver. Finally, we show an example of a spatially entangled nonclassical optical probe and an explicit receiver design—constructible using a single-photon source, beam splitters, and single-photon detectors—that in principle can read any number of *error-free* bits of information using a single transmitted photon. The probe is a single photon in a uniform superposition of multiple spatial modes, viz., a W state.

II. CAPACITY OF OPTICAL READING

The setup we consider is shown in Fig. 2. Each memory pixel is a reflective surface that can modulate the incident optical mode(s) by a power attenuation factor $\eta_m \in [0, 1]$ and/or a (carrier) phase shift $\theta_m \in (0, 2\pi]$. A K -mode transmitter interrogates each memory pixel. Each pixel acts like a beam splitter, such that the k th return mode from the m th pixel is given by $\hat{a}_R^{(m,k)} = \sqrt{\eta_m} e^{j\theta_m} \hat{a}_S^{(m,k)} + \sqrt{1 - \eta_m} \hat{a}_E^{(m,k)}$, where the $\{\hat{a}_S^{(m,k)}\}$ are the transmitter (signal) modes and the environment modes, $\{\hat{a}_E^{(m,k)}\}$, are taken to be in their

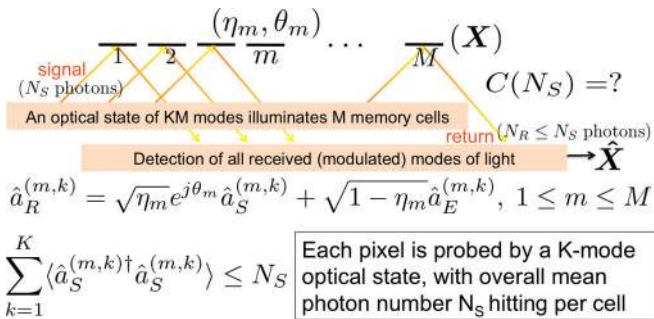


FIG. 2. (Color online) Schematic of an optical memory that uses passive linear-optic reflective encoding. M memory pixels are shown. Each pixel can modulate the spatial mode of the incident probe light by a power attenuation $\eta_m \in [0, 1]$ and/or a (carrier) phase shift $\theta_m \in (0, 2\pi]$.

respective vacuum states, implying no excess noise. We impose a mean photon-number constraint on the transmitter, $\sum_{k=1}^K \langle \hat{a}_S^{(m,k)\dagger} \hat{a}_S^{(m,k)} \rangle \leq N_S$ photons per pixel. In what follows we address the following two canonical questions:

(1) **Capacity**—How many bits of information can be reliably encoded and read per memory pixel, $C(N_S)$ bits/pixel, as a function of the average photon number spent to interrogate a pixel, N_S , when there are no constraints on the length of the code, the transmitter state, and the receiver measurement? The PIE is the number of bits read per signal photon, given by $C(N_S)/N_S$ bits/photon. As is true for most capacities, reading data at a rate $R < C(N_S)$ bits/pixel at a probability of word error $P_e^{(M)} \rightarrow 0$, may require coding over $M \rightarrow \infty$ many pixels and employing a JDR over infinitely many pixels.

(2) **Error exponent**—What is the minimum number of pixels M required (length of code and JDR) to attain a certain PIE, such that $P_e^{(M)} \leq \epsilon$?

For both of the preceding performance metrics, we would also like to know by how much can nonclassical states of light and/or nonstandard optical receivers (including JDRs) outperform a coherent-state probe and the standard optical receivers (homodyne, heterodyne, and direct detection).

At this point, readers who are familiar with the Holevo capacity of bosonic channels [18], might see the correspondence between the above problem and the problem of finding the capacity $C_{\text{comm}}(N_S)$ (bits/use) of a single-mode pure-loss bosonic channel when N_S photons are transmitted, on average, per channel use. It is well known that the Holevo capacity for that channel— $C_{\text{comm}}(N_S) = g(\eta N_S)$ bits/use, where $g(x) = (1+x) \log_2(1+x) - x \log_2(x)$ and η is the channel's transmissivity—can be achieved using coherent-state modulation and a joint-detection receiver. It is easy to see that the capacity of optical reading, $C(N_S) \leq C_{\text{comm}}(N_S)$, because the light reflected from M memory pixels can be regarded as an M -mode code word. It is *not* obvious, however, that equality holds, i.e., $C(N_S) = C_{\text{comm}}(N_S)$, nor is it clear that a coherent-state probe can attain the reading capacity. It turns out that $C(N_S) = g(\eta N_S)$, where η is now the average reflectivity of the encoded pixels, is *only* possible for lossless optical reading, viz., phase-only encoding with $\eta = 1$. Furthermore, even in the lossless case, $C(N_S) = g(N_S)$ *cannot* be achieved with coherent states [17,19]. Thus, despite the similarities of optical communication and optical reading, the latter problem is more constrained than the former, because its modulation and coding happen passively at the pixels, with the transmitter being ignorant of the information to be modulated on the probe light. In communication—for which the information to be modulated and coded is available to the transmitter—the spate of recent work on Holevo capacity-achieving codes [20,21] and joint-detection receivers [16,22–24] has yet to yield an efficient Holevo-capacity-achieving code and a structured optical design for its JDR. Surprisingly, we exhibit an explicit capacity-achieving system for lossless optical reading.

To focus on the fundamental aspects of the capacity and error-exponent questions, we assume that there is no return-path loss of the probe light (except for any loss due to amplitude modulation by the memory pixels); no excess noise (such as noise due to detector imperfections or a thermal background); and a diffraction-limited transceiver

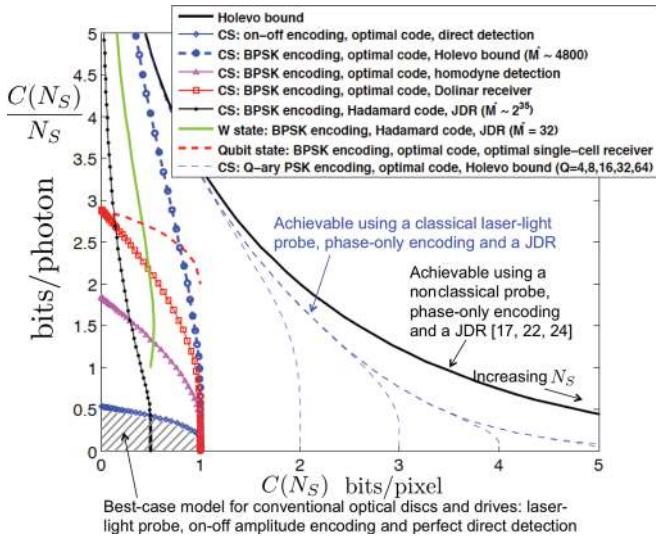


FIG. 3. (Color online) Photon information efficiency of optical reading (bits read per photon) vs the encoding efficiency (bits encoded per pixel) for various transmitter and receiver strategies. The gray-shaded area shows the Shannon limit of the performance achievable using an ideal laser-light probe, on-off amplitude encoding, and an ideal direct detection receiver—an overly optimistic model for how conventional optical drives read data from disks.

with spatially resolved pixels. There is a fundamental trade-off between optical reading’s photon efficiency (bits read per photon) and its encoding efficiency (bits encoded per pixel). This trade-off—for a variety of transmitter, encoding, and receiver techniques—is summarized in Fig. 3. High photon efficiency (hence, low encoding efficiency) is attained for a low-brightness transmitter (low N_S), whereas attaining high encoding efficiency (hence, low photon efficiency) requires a bright transmitter (high N_S). The gray-shaded area in Fig. 3 corresponds to the best performance achievable using conventional techniques. The derivations of these trade-off curves are explained below. We focus on the high photon efficiency (low photon flux) regime in this paper. It is here that the advantage of joint detection is the most pronounced. We defer consideration of the high encoding efficiency regime to the sequel [19] of the present work; it will be a long version of Ref. [17]. Finally, we also limit our scope in this paper to a single-mode transmitter, i.e., $K = 1$.

We begin by considering an idealized model for the standard CD or DVD drive, i.e., a laser-light probe, on-

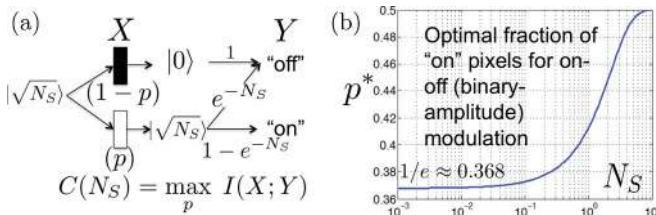


FIG. 4. (Color online) (a) The induced binary channel for a coherent-state probe, on-off pixel encoding, and shot-noise-limited direct detection. (b) The optimal fraction of “on” pixels p^* that maximizes the number of bits read per pixel $C(N_S)$, when mean photon number N_S is used to interrogate each memory pixel.

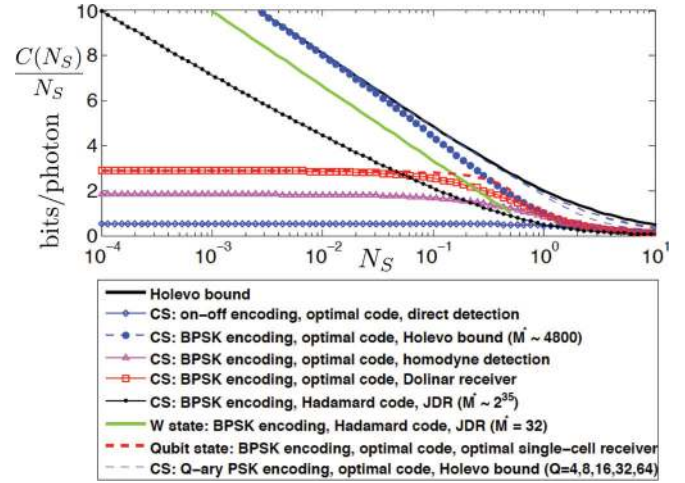


FIG. 5. (Color online) Photon information efficiency (PIE) vs the mean photon number N_S used to interrogate each memory pixel. CS denotes coherent state. is the minimum number of pixels needed to achieve 5 bpp at $P_e = 10^{-3}$.

off amplitude modulation, and a direct-detection receiver. Interrogation and detection of each pixel induces a binary asymmetric channel, as shown in Fig. 4(a). The Shannon capacity [25] of this channel is given by

$$C(N_S) = \max_{p \in (0,1)} I(X; Y) \quad (1)$$

$$= \max_{p \in (0,1)} [H(Y) - H(Y|X)] \quad (2)$$

$$= \max_{p \in (0,1)} [H(p(1 - e^{-N_S})) - pH(e^{-N_S})], \quad (3)$$

where $H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the binary entropy function. The optimal value of p that maximizes the mutual information $I(X; Y)$ is the fraction of “on” pixels in a capacity-achieving code, which is readily computed to be

$$p^*(N_S) = \frac{1}{(1 - e^{-N_S})[1 + 2H(e^{-N_S})/(1 - e^{-N_S})]}. \quad (4)$$

Figure 4(b) shows that $p^*(N_S) \rightarrow 0.5$ for $N_S \gg 1$. This is the regime in which a standard CD drive operates, wherein optimal codes have equal fractions of *on* and *off* pixels. On the other hand, $p^*(N_S) \rightarrow 1/e \approx 0.368$ for $N_S \ll 1$. The solid blue line in Fig. 5 plots the PIE, $C(N_S)/N_S$, as a function of N_S for on-off pixel modulation, a coherent-state probe, and direct detection. The PIE caps off, $C(N_S)/N_S \rightarrow 1/e \ln(2) \approx 0.53$ bits per photon (bpp) for $N_S \ll 1$. Thus, even with the optimal code (code words infinitely many pixels long), using on-off modulation, an ideal laser transmitter, and an ideal direct-detection receiver, no more than about 0.5 bits can be read per transmitted photon.

Let us now consider the binary phase-shift keyed (BPSK) modulation. Each memory pixel is a perfectly reflective pixel but some are etched $\lambda/2$ deeper into the surface of the disk, where λ is the center wavelength of the (quasimonochromatic) probe light. A coherent-state probe $|\sqrt{N_S}\rangle$ sent to interrogate the m th pixel gets reflected as $|\sqrt{N_S}\rangle$ or $|-\sqrt{N_S}\rangle$ depending upon whether that pixel’s phase is $\theta_m = 0$ or π . The conventional receiver to discriminate the states $\{|\sqrt{N_S}\rangle, |-\sqrt{N_S}\rangle\}$

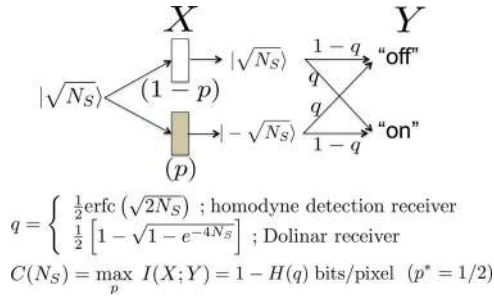


FIG. 6. (Color online) A binary symmetric channel is induced when a coherent-state probe $|\sqrt{N_S}\rangle$ interrogates each memory pixel, and the reflected light is detected by either a conventional homodyne receiver with a threshold detector or by the Dolinar receiver—a receiver that can attain the minimum probability of error for discriminating between two coherent states.

$\sqrt{N_S}\rangle$ uses homodyne detection, which results in a Gaussian-distributed measurement outcome β , with mean $\pm\sqrt{N_S}$ and variance $1/4$. The minimum error-probability postdetection processor is the threshold test, $\beta \geq 0 \Rightarrow \theta = 0$ and $\beta < 0 \Rightarrow \theta = \pi$, which induces a binary symmetric channel (BSC) with crossover probability $q_{\text{hom}} = \operatorname{erfc}(\sqrt{2N_S})/2$ (see Fig. 6), whose capacity is given by $C(N_S) = 1 - H(q_{\text{hom}})$ bits/pixel and is achieved for an equal prior ($p^* = 1/2$) for the two phase values. The minimum achievable error probability for discriminating a single copy of the two equally likely coherent states $\{|\sqrt{N_S}\rangle, |-\sqrt{N_S}\rangle\}$ is given by the Helstrom limit [26], $P_{e, \min} = [1 - \sqrt{1 - e^{-4N_S}}]/2$. This minimum probability of error can in principle be achieved exactly using the Dolinar receiver [27,28], which is a structured optical receiver design that uses a local time-varying optical feedback and high-speed ideal single-photon detection. The Dolinar receiver used with BPSK modulation induces a BSC with crossover probability $q_{\min} = P_{e, \min}$, and capacity $C(N_S) = 1 - H(q_{\min})$ bits/pixel. The magenta (dark gray) and red (gray) plots in Fig. 5 show the PIE for BPSK encoding with the homodyne and Dolinar receivers, which cap off at $4/\pi \ln(2) \approx 1.84$ bpp and $2/\ln(2) \approx 2.89$ bpp, respectively, for $N_S \ll 1$.

For a single $\{0, \pi\}$ binary phase-modulated pixel, of all (multimode) transmitter states with mean photon number N_S , the one that minimizes the probability of error is the single-mode ($K = 1$) *single-rail encoded* qubit state, $|\psi\rangle^S = \sqrt{1 - N_S}|0\rangle + \sqrt{N_S}|1\rangle$, which attains zero probability of error for $N_S \geq 1/2$, and $P_{e, \min, \text{QS}} = [1 - \sqrt{1 - [1 - 2N_S]^2}]/2$, for $N_S < 1/2$ [12]. Capacity is again given by the BSC capacity formula, $C(N_S) = 1 - H(P_{e, \min, \text{QS}})$ bits/pixel (see the red (gray)-dashed plot in Fig. 5). The resulting PIE caps off at $2/\ln(2) = 2.89$ bpp for $N_S \ll 1$. Note that the BPSK pixel modulation format achieves the minimum possible probability of error over all transmitters and receivers acting on reflection from single pixels and hence achieves higher capacity (and PIE) than what can be obtained via amplitude modulation alone [7]. Notwithstanding, the PIEs of all the cases considered above cap off below 3 bpp.

The classical information-carrying (Holevo) capacity of a quantum signaling alphabet was found by Holevo,

Schumacher, and Westmoreland [14,15]. The Holevo capacity of the pure-loss (vacuum-noise) optical channel with a mean received photon number per mode N_S is $g(N_S)$ bits/mode [18]. This capacity is achievable using a coherent-state code with symbols $|\alpha\rangle$ chosen in an independent, identically distributed (i.i.d.) manner from the isotropic Gaussian distribution, $p(\alpha) = e^{-|\alpha|^2/N_S}/\pi N_S$. Hence, for communicating classical data on a pure-loss optical channel, nonclassical transmitter states cannot achieve any higher capacity than coherent states. From the capacity theorem converse in Ref. [18]—treating the reflected light from the memory pixels as a modulated code word—and monotonicity of the $g(\cdot)$ function, the capacity of optical reading must satisfy the upper bound, $C(N_S) \leq g(N_S)$, for all single-mode probe states ($K = 1$). However, the reading problem has less encoding freedom than the communication transmitter, because its modulation must be passive (nonamplifying) at the pixels. That is why $C(N_S) = g(N_S)$ bits/pixel is not achievable for optical reading using a coherent-state transmitter [19]. However, we have shown that $C(N_S) = g(N_S)$ bits/pixel is achievable using a nonclassical transmitter [17,19] and a sequential-decoding quantum joint-detection receiver [23].

The black-dashed line in Fig. 5 shows the PIE of the Holevo bound $g(N_S)/N_S$. Note that unlike all the capacity results for on-off and binary-phase modulation with explicit pixel-by-pixel detection schemes considered above, the Holevo bound has no upper limit to the number of bits that can be read per expended photon. However, as the desired PIE increases, the mean photon number N_S used to interrogate each pixel must be lower, resulting in a lower data rate $C(N_S)$ (bits/pixel) read. Even though coherent states do not achieve the Holevo bound on reading capacity, a coherent-state probe can nevertheless approach $g(N_S)$ in the high-PIE ($N_S \ll 1$) regime when employed in conjunction phase modulation and the optimal JDR that makes a collective measurement over-return modes from many pixels, as we now show. The blue (gray)-dashed plots in Fig. 5 are the Holevo-limit PIEs of Q -ary phase-shift-keying (PSK) constellations used to encode the data for $Q = 2, 4, 8, 16, 32$. Because the PSK Holevo limit for any Q is an achievable rate [15], it is a lower bound to the reading capacity, i.e., $C(N_S) \geq C_{\text{PSK-Holevo}}(N_S)$, where

$$C_{\text{PSK-Holevo}}(N_S) = \max_{Q \geq 2} - \sum_{q=1}^Q y_q(N_S) \log_2 y_q(N_S),$$

with $\{y_q(N_S)\}$, $1 \leq q \leq Q$, being the probability distribution,

$$y_q(N_S) = \frac{1}{Q} \sum_{k=1}^Q e^{-N_S[1 - \cos(\frac{2\pi k}{Q})]} \cos \left[N_S \sin \left(\frac{2\pi k}{Q} \right) - \frac{2\pi k q}{Q} \right].$$

For $Q = 2$ (BPSK modulation), the Holevo capacity is given by $C_{\text{BPSK}}(N_S) = H((1 + e^{-2N_S})/2)$ bits/pixel. Its PIE is shown by the dark blue (gray)-dashed plot in Fig. 5, where it is seen to approach the Holevo limit $g(N_S)/N_S$ at low N_S . Thus, the gap between the PIE of BPSK modulation used with an optimal single-symbol receiver (solid red [gray] plot) and

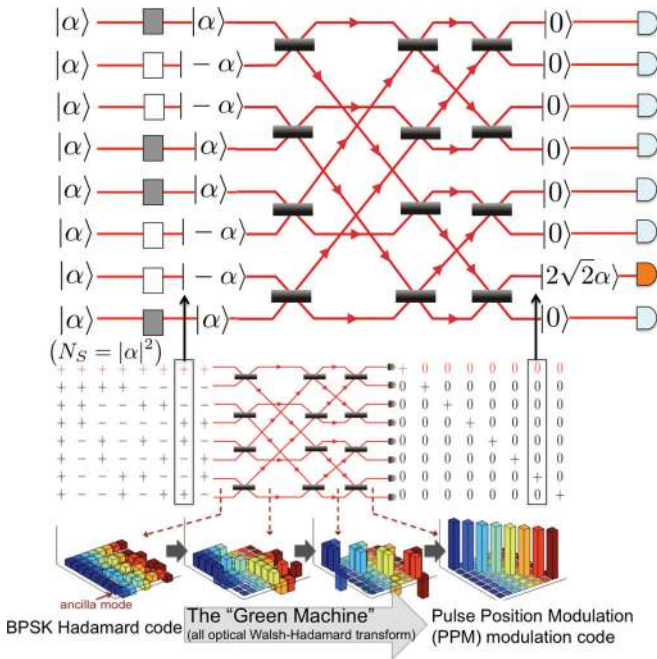


FIG. 7. (Color online) The Green Machine JDR. Each vertical column of + and - signs is a reflection from M binary-phase-coded memory pixels—a coherent-state BPSK code word from the Hadamard code with M pulses of mean photon number N_S each. Each of the M code words transforms into exactly one coherent state of mean photon number MN_S at one distinct output port of the optical circuit of $(M/2)\log_2(M)$ beam splitters. Under ideal conditions, a click at one of the M single-photon detectors identifies the reflected code word with no error, whereas a no-click leads to an *erasure* outcome, which induces the M -ary symmetric erasure channel shown in Fig. 8.

the Holevo limit of BPSK (dashed blue [gray] plot) can and must be bridged using a JDR.

The first explicit code-JDR pair for a BPSK alphabet that achieves *superadditive* capacity (i.e., higher capacity than what is achievable with the optimal single-symbol receiver for BPSK) was found by one of us recently in the context of communication [16], but that construct—which we now describe—also applies to optical reading. The Green Machine JDR for BPSK-modulated pixels and a coherent-state probe is depicted in Fig. 7. It uses a $(2^m, 2^m, 2^{m-1})$ binary Hadamard code to encode the binary phases on $M = 2^m$ pixels. The receiver comprises an interferometer made of $(M/2)\log_2(M)$ 50:50 beam splitters arranged in a format—first envisioned by R. R. Green as a classical decoding circuit for Hadamard codes [29]—that interferometrically mixes the modulated light from the M pixels, transforming the BPSK Hadamard code word, through $\log_2(M)$ stages of the Green Machine, into a spatial pulse-position-modulation (PPM) code. A coherent-state pulse with mean photon number MN_S appears at one of the M outputs, depending upon which of the M -pixel Hadamard code words the probe light interrogates. The output is detected by an array of M signal-shot-noise-limited single-photon detectors. This probe-code-JDR combination induces an M -input, $M + 1$ -output superchannel, shown in Fig. 8, whose

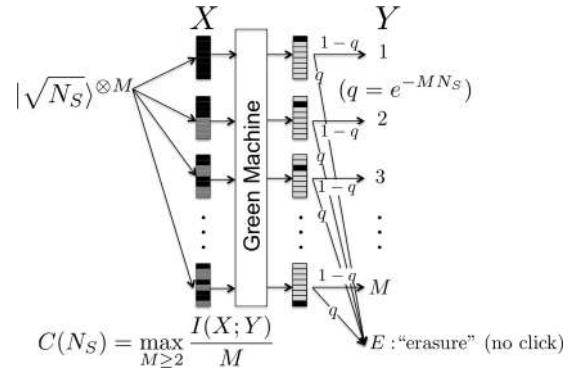


FIG. 8. The M -input, $M + 1$ -output channel induced by the coherent-state probe, binary-phase Hadamard coded memory, and the Green Machine JDR.

capacity (in bits/pixel) is given by

$$\begin{aligned} C_{\text{BPSK-Hadamard-JDR}}(N_S) &= \max_{M \geq 2} \frac{I(X; Y)}{M} = \max_{M \geq 2} \frac{\log_2(M)(1 - e^{-MN_S})}{M} \\ &= \frac{1}{\ln(2)} \left\{ N_S \ln\left(\frac{1}{N_S}\right) - N_S \ln\left[\ln\left(\frac{1}{N_S}\right)\right] + \dots \right\}, \quad (5) \end{aligned}$$

when $N_S \ll 1$. Here, the PIE-maximizing value of the code size M as a function of N_S is given by $M^* \approx -5/2N_S \ln(N_S)$, for $N_S \ll 1$. This PIE is plotted as the solid black line in Fig. 5. Unlike all the structured probe-receiver cases we have considered so far—in which the optical receiver measured the reflected light from each pixel individually—the PIE attained by the BPSK Hadamard code and the Green Machine JDR increases without bound as $N_S \rightarrow 0$. Note that this PIE is optimal to the leading-order term of the Holevo bound (both the unrestricted-modulation Holevo bound and the coherent-state-probe BPSK-encoding Holevo capacity) for $N_S \ll 1$:

$$C(N_S) = \frac{1}{\ln(2)} \left[N_S \ln\left(\frac{1}{N_S}\right) + N_S + \dots \right] \text{ bits/pixel.} \quad (6)$$

One can increase the photon efficiency slightly by using the $(2^m - 1, 2^m, 2^{m-1})$ Hadamard code, thereby using one less ($M = 2^m - 1$) pixel and retaining a local-oscillator reference at the transmitter for use as a local input into the Green Machine. Note that the achievable capacity in Eq. (5) and all the coherent-state structured-receiver capacities given above are Shannon capacities of the respective discrete memoryless channels induced by the choice of the probe-code-receiver combination. Hence, in order to achieve error-free reading at a rate close to these capacities (in bits/pixel), a suitable Shannon-capacity-approaching outer code—such as a Reed Solomon code—will be required.

Now, let us keep the same BPSK modulation and Hadamard code but consider using a spatially entangled nonclassical probe state, the W state, instead of a coherent state. This probe sends exactly one photon in a coherent superposition of M spatial modes,

$$|W_M\rangle \equiv \frac{|10\dots 0\rangle + |01\dots 0\rangle + \dots + |00\dots 1\rangle}{\sqrt{M}}, \quad (7)$$

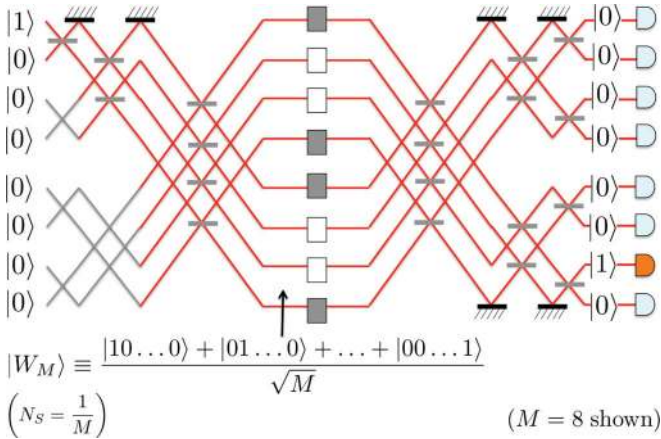


FIG. 9. (Color online) The W -state transmitter, generating the $M = 8$ mode W state, interrogates M binary-Hadamard phase-coded pixels. The wave function of the single photon evolves through the receiver stages, eventually coalescing into the single-photon Fock state $|1\rangle$ at one of the M outputs of the receiver, depending upon which one of the M Hadamard code words the transmitter state interrogated.

to interrogate M memory pixels, where M is taken to be even. It can be prepared using a single-photon source (generating a one-photon Fock state $|1\rangle$) split via an array of 50:50 beam splitters as shown in Fig. 9. Recently, it was shown how to perform fast heralded generation of the W state, and other complicated mode-shaped single photon states, by indirectly tailoring the mode of the single photon via amplitude modulation of the classical pump field driving a spontaneous parametric downconversion process [30]. Reflection of the W state by the Hadamard-phase-coded pixels causes the $+$ signs in the W -state superposition corresponding to the pixels with $\theta = \pi$ to flip to $-$ signs. Let the memory-modulated state for code word m be $|W_M^{(m)}\rangle$, for $1 \leq m \leq M$. Because any pair of code words from the Hadamard code differ in exactly $M/2$ positions, the $\{|W_M^{(m)}\rangle\}$ are mutually orthogonal quantum states; i.e., $\langle W_M^{(m_1)} | W_M^{(m_2)} \rangle = \delta_{m_1, m_2}$. Therefore, it is possible, in principle, to discriminate these M modulated states with zero probability of error. An explicit receiver that accomplishes this zero-error discrimination is shown in Fig. 9. The wave function of the single photon evolves through the $\log_2(M)$ receiver stages, eventually coalescing into the single-photon Fock state $|1\rangle$ at one of the M outputs of the beam-splitter circuit, depending upon which one of the M Hadamard code words the transmitter state interrogated. A single-photon Fock state $|1\rangle$ generates a click with probability 1 when detected by an ideal single-photon detector (unlike a coherent state $|\beta\rangle$, which generates a click with probability $1 - e^{-|\beta|^2}$ under ideal conditions). Therefore, the W -state transceiver reads $\log_2(M)$ bits of information *error-free*—i.e., without any further outer coding—using just one transmitted photon, with no upper limit on M . Clearly, $N_S = 1/M$. Therefore, capacity is given by

$$C_{W\text{-state}}(N_S) = N_S \log_2\left(\frac{1}{N_S}\right) \text{ bits/pixel.} \quad (8)$$

This capacity has the same low- N_S leading-order term as the Holevo limit and the coherent-state Green Machine JDR. The PIE for the W state is exactly $\log_2(1/N_S)$ bpp, i.e., a

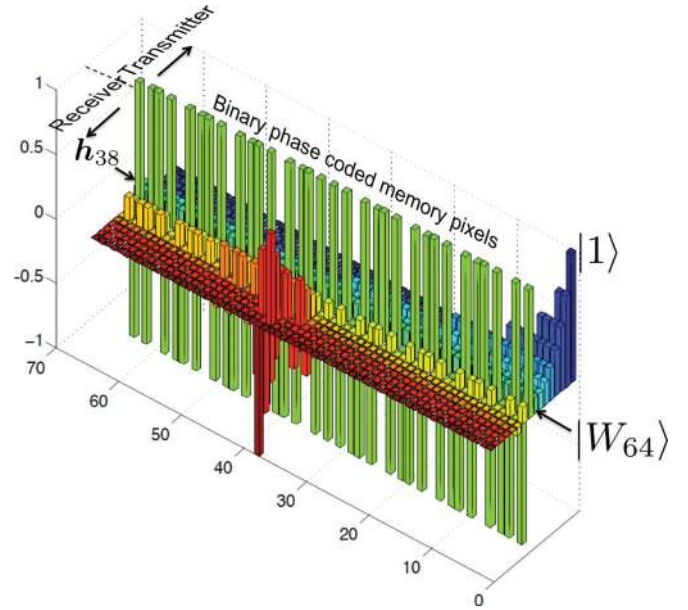


FIG. 10. (Color online) An $M = 64$ example of W -state probability-amplitude evolution during the encoding and decoding phases of optical reading. The vertical axis denotes the amplitude and binary phase of the photon wave function. Positive (upward from 0) denotes 0 phase and negative (downward from 0) denotes π phase. The green (gray) vertical bars depict the 38th of the BPSK Hadamard code words, h_m , $1 \leq m \leq 64$, using the above sign convention for 0 and π phases. A single-photon Fock state $|1\rangle$ is shown to go through the $\log_2(M) = 8$ stages of the encoding circuit, shown in Fig. 9, to form the equal-superposition W state $|W_{64}\rangle$, which undergoes phase modulation at the memory pixels (green [gray] bars). The modulated W state is shown to go through the eight stages of the optical receiver circuit, also shown in Fig. 9, eventually forming a single-photon Fock state $|1\rangle$ (with an unimportant phase) at the correct (38th) output port, which is then detected without error by an ideal single-photon detector.

straight line when plotted versus N_S on a logarithmic scale (see the green [gray] line in Fig. 5). Figure 10 shows an $M = 64$ example of the single photon's probability-amplitude evolution during the encoding and decoding phases of optical reading using a W state.

III. ERROR EXPONENT OF QUANTUM READING

All the results obtained in Sec. II are Holevo or Shannon capacities. Thus, achieving a reliable rate of reading—i.e., reading information such that the probability of code-word error $P_e^{(M)} \leq \epsilon$ for some low-enough threshold ϵ —at any given rate $R < C(N_S)$ bits/pixel would require an optimal outer code for all the Shannon-capacity structured-receiver cases considered and would require an optimal code as well as an optimal JDR for the Holevo-capacity results. The W -state example does not require an outer code, because of its zero-error receiver.

Reading capacity gives a crucial information-theoretic perspective, namely, the fundamental limit on achievable rates at which data can be read. However, capacity alone only specifies the maximum achievable rate. It provides no information about the coding and receiver complexity required to read data

reliably at any achievable rate. Hence, a stronger form of the channel coding theorem has been pursued to determine the behavior of the minimum code-word-error probability, $P_e^{(M)}$, as a function of the code-word length (number of pixels) M and the data rate R (bits/pixel), for all rates $R < C$ —both for classical channels (where C is the channel's Shannon capacity) [31,32] as well for quantum channels (where C is the channel's Holevo capacity) [33,34]. We define the reliability function or the *error exponent* for optical reading as [31]

$$E(R) \equiv \limsup_{M \rightarrow \infty} \frac{-\ln [P_e^{\text{opt}}(R, M)]}{M}, \quad \forall R < C(N_S), \quad (9)$$

where $P_e^{\text{opt}}(R, M)$ is the average word-error probability for the optimal block code of M pixels and rate R . The error exponent describes how quickly the error probability decays as a function of M , and hence serves to indicate how difficult it may be to achieve a certain level of reliability in reading at a given rate below the capacity. Although it is difficult to exactly evaluate $E(R)$, its classical lower bound is available due to Gallager [32]. This lower bound to the error exponent is known as the random-coding lower bound and has been used to estimate the code-word length required to achieve a prescribed error probability for various communication settings. Burnashev and Holevo found the random-coding bound and the expurgated bound for sending classical data on quantum channels, both being lower bounds to $E(R)$ for a pure-state alphabet [33], and later generalized the expurgated bound to a mixed-state alphabet [35]. The best-known lower bound to the quantum channel's reliability function $E(R)$ was reported by Hayashi [36]. For classical channels, there exists an upper bound (the sphere-packing bound) which coincides with $E(R)$ for high rates, i.e., for rates R close to the Shannon capacity, C , and thus gives the exact expression for $E(R)$. Until very recently, no useful upper bound for $E(R)$ had been known for the quantum case. That changed, however, when Dalai reported the sphere-packing bound on the error exponent for sending classical data over a quantum channel [34]. Dalai's upper bound to $E(R)$ for the quantum channel coincides with the random-coding lower bound at high rates, thereby yielding the true value of $E(R)$ in this region. More work needs to be done in the low-rate regime, in order to fully determine the error exponent $E(R)$ for a quantum channel for all rates R below the Holevo capacity.

In order to compare the error-exponent performance of various transceivers we proposed in Sec. II, let us choose a PIE goal of 5 bpp and probability of word-error threshold $\epsilon = 10^{-3}$.

A. Coherent-state probe: optimal code, optimal JDR

We now estimate the number of pixels M required to achieve 5 bpp with $P_e^{(M)} = 10^{-3}$ using a coherent-state transmitter and the optimum code-JDR pair. We evaluate the Burnashev-Holevo lower bound to the error exponent, $E_{\text{LB}}(N_S, R) \leq E(N_S, R)$, for the states $\{|\sqrt{N_S}\rangle, |-\sqrt{N_S}\rangle\}$, for which $\langle -\sqrt{N_S} | \sqrt{N_S} \rangle = e^{-2N_S}$ (Sec. 4 of Ref. [33]). Figure 11 shows contours of constant $M_{\text{UB}} \equiv -\ln(\epsilon)/E_{\text{LB}}(N_S, R)$ in the PIE (R/N_S) vs N_S plane for $\epsilon = 10^{-3}$. At $R/N_S = 5$ bpp, we find that $M_{\text{UB}} = 4800$. Therefore, in order to attain 5 bpp at $P_e^{(M)} \leq 10^{-3}$, the

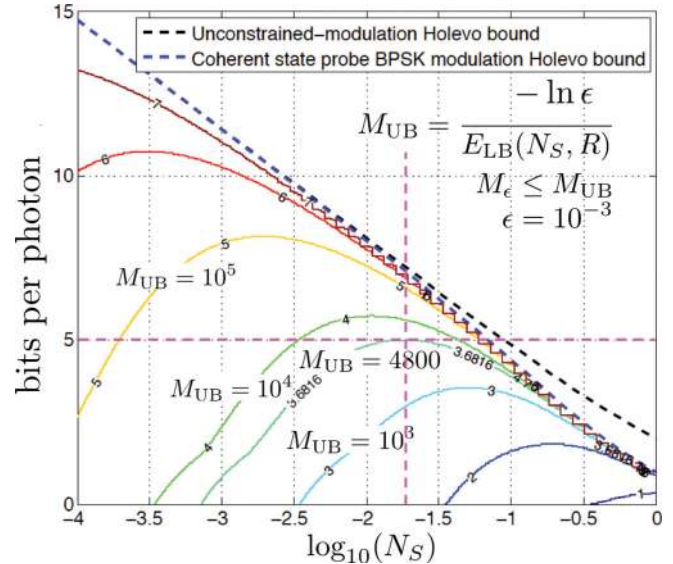


FIG. 11. (Color online) Contours of constant $M_{\text{UB}} \equiv -\ln(\epsilon)/E_{\text{LB}}(N_S, R)$ —the upper bound to the number of pixels required to achieve 5 bpp with a 10^{-3} word-error probability found from the Burnashev-Holevo random-coding bound for a pure-state quantum channel—plotted in the PIE (R/N_S) vs N_S plane. A coherent-state probe interrogating a binary-phase coded memory and an optimal JDR are assumed.

minimum number of pixels required satisfies $M \leq 4800$. Given that the rate is about 2/3 of capacity at the point where 5 bpp is barely reached (see the dashed magenta [gray] lines in Fig. 11), the random-coding bound is likely to be a fairly good estimate of the actual number of pixels required for an optimal code-JDR pair. A tighter upper bound and a tight lower bound on M may be obtainable by using the recent results on the second-order asymptotic analysis of the quantum relative entropy [37,38].

B. Coherent-state probe: Hadamard code, Green Machine JDR

The probability of word error for this probe-code-JDR combination is given by the probability of erasure multiplied by the probability the erasure is mapped to an incorrect code word, $P_e^{(M)} = (M-1)e^{-MN_S}/M$. It follows that the PIE obeys $C(N_S)/N_S = \log_2(M)(1 - e^{-MN_S})/MN_S$ bpp, from which it is easy to deduce that achieving 5 bpp at $P_e^{(M)} \leq 10^{-3}$ will require $M \approx 2^{35}$ pixels. This pixel number is many orders of magnitude higher than what is required by the optimal code-JDR pair.

C. W-state probe: Hadamard code, JDR

The W -state transmitter, along with a Hadamard binary-phase code and the JDR shown in Fig. 9, can read $\log_2 M$ bits using one transmitted photon at $P_e^{(M)} = 0$. Therefore, to achieve 5 bpp, at $P_e^{(M)} \leq 10^{-3}$, an $M = 32$ pixel memory suffices. This demonstrates the *huge* error-exponent benefit enjoyed by a quantum (spatially entangled) transmitter in comparison with the coherent-state probe—even when the as-yet-unknown optimal JDR for a capacity-achieving coherent-state code may become available.

IV. CONCLUSIONS AND DISCUSSION

We showed that using a coherent-state probe, on-off amplitude modulation, and signal-shot-noise-limited direct detection (a highly optimistic model for conventional CD and DVD drives), one cannot read any more than about 0.5 bits per transmitted photon. We then showed that a coherent-state transmitter, in conjunction with a binary-phase-shift-keyed encoding, can read an unlimited number of bits reliably per expended photon, if nonstandard joint-detection measurements are allowed at the receiver. This capacity performance of coherent states approaches the Holevo bound to capacity in the high-photon-information-efficiency low-photon-flux regime. However, with a coherent-state source and binary phase encoding, if the receiver is constrained to detect the reflected light from each memory pixel one at a time followed by classical signal processing—all conventional optical receivers fall in this category—then the highest photon efficiency achievable caps off at about 2.89 bits per photon. Thus, joint detection receivers are needed to bridge the gap to the Holevo capacity, which allows for unbounded photon efficiency for optical reading. We exhibited one example of a BPSK code-JDR pair that can bridge part of that gap and attain an unbounded PIE. However, this example has a poor error-exponent performance. In particular, in order to attain 5 bpp at a word-error probability $P_e^M \leq 10^{-3}$, it requires coding over $M \approx 2^{35}$ memory pixels, unlike the $M \approx 4800$ pixels required by the unknown optimal code-JDR pair to attain 5 bpp and $P_e^M \leq 10^{-3}$ with a coherent-state probe and BPSK modulation. Finally, we showed that a nonclassical W -state probe can read $\log_2(M)$ bits of data using a single photon in an M -mode spatially entangled uniform-superposition state. That performance is realized with a BPSK Hadamard code and a structured interferometric receiver which uses a linear-optical circuit of beam splitters and single-photon detectors. It attains 5 bpp and $P_e^M = 0$ with just $M = 32$ pixels, demonstrating the huge error-exponent advantage afforded by a quantum transmitter state.

That the W -state transmitter can read any number of bits of information using just one photon should come as no surprise. Consider the thought experiment shown in Fig. 12. A perfectly reflective mirror encodes information using M well-resolved angular orientations, such that a well-collimated

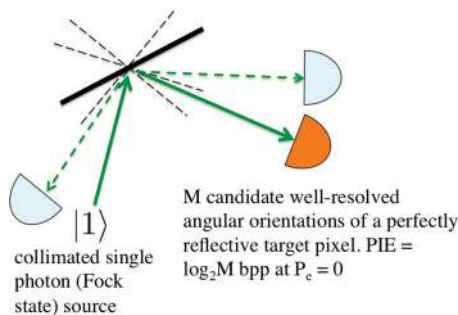


FIG. 12. (Color online) M angular positions of a perfectly reflective mirror can encode $\log_2 M$ bits of information that can be read error free, in principle, by a well-collimated single-photon Fock state source and an array of unity-detection-efficiency single-photon detectors.

single-photon beam, reflected by the mirror, is detected via an array of single-photon detectors, one matched to each of the mirror's angular positions. Like the W -state transceiver, this arrangement reads $\log_2(M)$ bits of information using one probe photon. These angular well-resolved orthogonal modes can be replaced by any set of M orthogonal space-time-polarization modes of light that the target (memory) can excite using the incident single-photon state. For the W -state example, the orthogonal modes that the spatially entangled photon excites are a set of spatially overlapping mutually orthogonal spatial modes corresponding to the binary Hadamard code words. This is quite similar to the mutually orthogonal chip wave forms of a spread-spectrum code-division multiple-access (CDMA) system.

Before concluding, it is in order to comment briefly on the effect that loss has on optical reading. In a practical setting, loss would be incurred at various points in the reading setup: at the transmitter that generates the probe light, in the transmission to the memory pixel, in absorption and scattering of the probe light at the pixel, in collecting the reflected light at the receiver, and in the subunity quantum efficiency of the single-photon detector. It turns out that the capacities of all the coherent-state systems we have considered in this paper degrade gracefully with loss; i.e., these capacities have the same formulas as given in the paper for no loss with the average number of transmitted photons N_S replaced by the average number of detected photons κN_S , where $1 - \kappa \in (0, 1]$ is the end-to-end loss. Furthermore, the number of pixels M needed to get a desired number of bits per *detected* photon for a given word-error probability does not change from what we found for the lossless case for bits per *transmitted* photon. For example, consider the binary-phase Hadamard code and a coherent-state probe, with the Green Machine JDR. The resulting word-error probability in the lossy scenario is $P_e^{(M)} = (M - 1)e^{-\kappa M N_S} / M \approx e^{-\kappa M N_S}$ for $M \gg 1$. So, $P_e^{(M)} = 10^{-3}$ requires $\kappa M N_S \approx 7$ photons, and since PIE $\approx \log_2(M) / \kappa M N_S$ bits per *detected* photon (bpdp), attaining 5 bpdp requires $M \approx 2^{5 \times 7} = 2^{35}$ pixels. The *single-shot* W -state transceiver is able to attain $P_e^{(M)} = 0$ for the binary-phase Hadamard code and PIE = $\log_2(M)$ bpp using one photon in the lossless case, thereby attaining 5 bpp using $M = 2^5 = 32$ pixels. However, the performance of the W -state transceiver degrades rapidly with loss, smoothly transitioning to that of the coherent-state and Green Machine JDR for high loss. The W state has an erasure probability equal to $1 - \kappa$. Assuming we send K copies of the W state towards the same set of Hadamard-coded pixels, and that we randomly assign a code word to every erasure, we are left with a word-error probability $P_e^{(M)} = (M - 1)(1 - \kappa)^K / M \approx e^{-\kappa K}$, for $M \gg 1$, $K \gg 1$. PIE in bits per detected photons is then PIE $\approx \log_2(M) / \kappa K$. Thus, to get to 5 bpdp with $P_e^{(M)} = 10^{-3}$ when $\kappa \ll 1$ we need $M \approx 2^{35}$ pixels, just as we have for the coherent-state probe. For a single-shot W -state transmission, attaining $P_e^{(M)} = 10^{-3}$ requires $\kappa \geq 0.999$, an extraordinarily demanding task considering that single-photon detectors with 99.9% quantum efficiency have yet to be built and there are many other sources of loss in the optical reading setup.

Finally, an interesting thing to note is that our W -state system is a special case of the Aaronson-Arkhipov (AA)

boson-sampling model [39], which inputs $\sim\sqrt{M}$ single photons in independent spatial modes into an M -mode passive linear-optic circuit implementing a unitary mode transformation $\hat{\mathbf{a}}_{\text{out}} = U\hat{\mathbf{a}}_{\text{in}}$, followed by ideal photon counting at that transformation's M output ports. The AA model was shown to be able to efficiently solve a sampling problem—that of sampling from a probability distribution comprised of the permanents of a set of matrices derived from U —a problem believed to be classically hard. The AA model, however, is not known to subsume universal quantum computation. A recent paper reported evidence supporting the proposition that a lossy AA system, or an AA system with mode mismatch in the linear-optic mode transformation, is likely to be classically hard to simulate and might thereby retain some quantum power [40]. This leads us to speculate that a multiphoton multimode transmitter could be more resilient to loss than the W state, and hence outperform coherent states in optical reading even in the presence of loss.

Reference [19] will address the capacity of optical reading at all values of the probe photon number constraint N_S . There we will show that not only do quantum probes achieve a higher error exponent, they can get a fundamentally higher capacity in the high spectral-efficiency ($N_S \gg 1$) regime. In [19] we will also consider the capacity of assisted reading,

i.e., when the transmitter retains idler modes $\{\hat{a}_I^{(m,k)}\}$ at the transmitter that are entangled with the signal modes $\{\hat{a}_S^{(m,k)}\}$ which were sent towards the pixel and joint detection is performed over the retained and returned modes. This arrangement is then the optical-reading version of quantum illumination, which has been previously studied for target detection [41] and eavesdropping-immune communication [42]. The ultimate capacity and error-exponent performance of multimode transmitters remain subjects of ongoing work.

ACKNOWLEDGMENTS

The authors thank Ranjith Nair, Brent J. Yen, Zachary Dutton, Mark M. Wilde, Stefano Pirandola, and Jonathan L. Habib for useful discussions. The authors thank Marco Dalai, Stefano Pirandola, and Peter P. Rohde for useful comments on a draft. S.G. was supported by the DARPA Information in a Photon (InPho) program under Contract No. HR0011-10-C-0162. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressly or implied, of the Defense Advanced Research Projects Agency or the US Government. J.H.S. acknowledges support from the ONR Basic Research Challenge Program.

-
- [1] K. Censor and T. Etzion, *IEEE Trans. Inf. Theory* **IT-52**, 5128 (2006).
 - [2] D. Carter, *Platinum Metals Rev.* **54**, 53 (2010).
 - [3] J. H. Shapiro, *Phys. Scripta* **T48**, 105 (1993).
 - [4] A. Acín, *Phys. Rev. Lett.* **87**, 177901 (2001).
 - [5] G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, *Phys. Rev. Lett.* **87**, 270404 (2001).
 - [6] S. Pirandola, *Phys. Rev. Lett.* **106**, 090504 (2011).
 - [7] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, *New J. Phys.* **13**, 113012 (2011).
 - [8] O. Hirota, arXiv:1108.4163v2 [quant-ph].
 - [9] C. Invernizzi, M. G. A. Paris, and S. Pirandola, *Phys. Rev. A* **84**, 022334 (2011).
 - [10] R. Nair and B. J. Yen, *Phys. Rev. Lett.* **107**, 193602 (2011).
 - [11] R. Nair, *Phys. Rev. A* **84**, 032312 (2011).
 - [12] R. Nair, B. J. Yen, S. Guha, J. H. Shapiro, and S. Pirandola, *Phys. Rev. A* **86**, 022306 (2012).
 - [13] M. Dall'Arno, A. Bisio, G. M. D'Ariano, M. Miková, M. Ježek, and M. Dušek, *Phys. Rev. A* **85**, 012308 (2012).
 - [14] A. S. Holevo, *Problemy Peredachi Informatsii* **15**, 3 [Problems of Information Transmission (USSR) **15**, 247] (1979).
 - [15] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, *Phys. Rev. A* **54**, 1869 (1996).
 - [16] S. Guha, *Phys. Rev. Lett.* **106**, 240502 (2011).
 - [17] S. Guha, Z. Dutton, R. Nair, J. H. Shapiro, and B. J. Yen, OSA Frontiers in Optics/Laser Science Conference 2011, San Jose, CA, USA (unpublished).
 - [18] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, *Phys. Rev. Lett.* **92**, 027902 (2004).
 - [19] S. Guha, R. Nair, B. J. Yen, J. H. Shapiro, and Z. Dutton (unpublished).
 - [20] M. M. Wilde and S. Guha, *IEEE Trans. Inf. Theory* **59**, 1175 (2013).
 - [21] S. Guha and M. M. Wilde, in *Proceedings of the 2012 IEEE International Symposium on Information Theory (ISIT 2012)*, Cambridge, MA, USA, 2012, 1–6 July 2012 (IEEE, Piscataway, 2012), pp. 546–550.
 - [22] S. Lloyd, V. Giovannetti, and L. Maccone, *Phys. Rev. Lett.* **106**, 250501 (2011).
 - [23] M. M. Wilde, S. Guha, S. H. Tan, and S. Lloyd, in *Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012*, Cambridge, MA, USA (IEEE, Piscataway, 2012), pp. 551–555.
 - [24] H. W. Chung, S. Guha, and L. Zheng, in *Proceedings of the 2011 IEEE International Symposium on Information Theory, St. Petersburg, Russia* (IEEE, Piscataway, 2011).
 - [25] C. E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
 - [26] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
 - [27] S. J. Dolinar, Ph.D. thesis, Massachusetts Institute of Technology, 1976.
 - [28] R. L. Cook, P. J. Martin, and J. M. Geremia, *Nature (London)* **446**, 774 (2007).
 - [29] R. R. Green, *JPL Space Programs Summary* 37–39, **IV** (1966); 37–53, **III** (1968).
 - [30] K. G. Köprülü, Y.-P. Huang, G. A. Barbosa, and P. Kumar, *Optics Lett.* **36**, 1674 (2011); K. G. Köprülü, G. A. Barbosa, and P. Kumar, *Quantum Electronics and Laser Science Conference (QELS)*, Baltimore, Maryland, 22 May 2005 (Optical Society of America, Washington, DC, 2005).
 - [31] C. E. Shannon, *Bell Syst. Tech. J.* **38**, 611 (1959).
 - [32] R. G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968).

- [33] M. V. Burnashev and A. S. Holevo, *Probl. Peredachi Inf.* **34**, 3 (1998).
- [34] M. Dalai, in *Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012, Cambridge, MA, USA* (IEEE, Piscataway, 2012), pp. 160–164.
- [35] A. S. Holevo, *IEEE Trans. Inf. Th.* **46**, 2256 (2000).
- [36] M. Hayashi, *Phys. Rev. A* **76**, 062301 (2007).
- [37] K. Li, Quantum Information Processing 2012, Beijing, China (unpublished).
- [38] M. Tomamichel and M. Hayashi, Quantum Information Processing 2012, Beijing, China (unpublished).
- [39] S. Aaronson and A. Arkhipov, in *Proceedings of 43rd ACM Symposium on Theory of Computing STOC, San Jose, CA* (ACM, New York, NY, 2011), pp. 333–342.
- [40] P. P. Rohde and T. C. Ralph, *Phys. Rev. A* **85**, 022332 (2012).
- [41] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, *Phys. Rev. Lett.* **101**, 253601 (2008).
- [42] J. H. Shapiro, *Phys. Rev. A* **80**, 022320 (2009).