

Achieving minimum-error discrimination of an arbitrary set of laser-light pulses

Marcus P. da Silva, Saikat Guha, and Zachary Dutton

Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, Massachusetts 02138, USA

(Received 10 September 2012; published 23 May 2013)

Laser light is widely used for communication and sensing applications, so the optimal discrimination of coherent states—the quantum states of light emitted by an ideal laser—has immense practical importance. Due to fundamental limits imposed by quantum mechanics, such discrimination has a finite minimum probability of error. While concrete optical circuits for the optimal discrimination between two coherent states are well known, the generalization to larger sets of coherent states has been challenging. In this paper, we show how to achieve optimal discrimination of any set of coherent states using a resource-efficient quantum computer. Our construction leverages a recent result on discriminating multicopy quantum hypotheses [Blume-Kohout, Croke, and Zwolak, arXiv:1201.6625]. As illustrative examples, we analyze the performance of discriminating a ternary alphabet and show how the quantum circuit of a receiver designed to discriminate a binary alphabet can be reused in discriminating multimode hypotheses. Finally, we show that our result can be used to achieve the quantum limit on the rate of classical information transmission on a lossy optical channel, which is known to exceed the Shannon rate of all conventional optical receivers.

DOI: [10.1103/PhysRevA.87.052320](https://doi.org/10.1103/PhysRevA.87.052320)

PACS number(s): 03.67.Lx, 03.67.Ac, 03.67.Hk, 42.50.Dv

I. BACKGROUND

Helstrom provided a set of necessary and sufficient conditions on the measurement that yields the minimum average probability of error in discriminating $K \geq 2$ distinct quantum states [1]. However, for optical state discrimination, this mathematical specification of measurement operators does not usually translate into an explicit receiver specification realizable using standard optical components, thus leaving a gap between the minimum-error probability (the *Helstrom limit*) and the minimum achievable by conventional measurements, e.g., homodyne, heterodyne, and direct detection.

Dolinar proposed a receiver that achieves the Helstrom limit exactly for discriminating any two coherent-state signals [2–4]. The receiver works by applying one of two time-varying optical feedback wave forms to the laser pulse being detected and instantaneously switching between the two feedback signals at each click event at a shot-noise-limited photon counter. More recently [5], it has been shown that an arbitrary multimode binary projective measurement can be implemented using adaptive linear-optic feedback and photon counting, thereby subsuming the Dolinar receiver.

For discriminating multiple ($K > 2$) coherent states, no optical receiver that achieves the Helstrom bound has been proposed, although several suboptimal receivers have been proposed to discriminate more than two coherent-state signals [6,7] and implemented [8], improving over the performance of conventional receivers. Much like the receiver in Ref. [5], each one of these suboptimal receivers operates via a common philosophy: that of *slicing* a coherent-state pulse into smaller coherent states, detecting each slice via photon counting after coherent addition of a local field, and feeding forward the detection outcome to the processing of the next slice, as illustrated in Fig. 1(a).

Attaining the quantum-limited channel capacity of an optical channel to carry classical information—the *Holevo limit*—requires joint detection over long coherent-state code words [9]. However, recent work has shown that even a joint-detection receiver involving the most general coherent-state

feedback, passive linear optics, and photon counting *cannot* attain the Holevo limit [10]. This proves that lasers, passive linear optics, and photon counting (the resources used by the Dolinar receiver) are not sufficient for general minimum-error optical state discrimination, unlike the binary-discrimination case.

II. DISCRIMINATING MULTIPLE COHERENT STATES

Our main result, the description of an optimal receiver for K -ary coherent-state discrimination, relies on two observations.

The first observation is that quantum-limited performance of any processing of an ensemble of K linearly independent pure states, $\mathcal{A} = \{|\alpha_j\rangle\}$, $1 \leq j \leq K$, is completely described by the Hermitian Gram matrix Γ , whose elements are the inner products $\gamma_{jk} \equiv \langle \alpha_j | \alpha_k \rangle$. Therefore, by a simple dimensionality argument, there must exist a unitary map $U_{\mathcal{A}}$ that maps the state ensemble \mathcal{A} to an ensemble of states of $\lceil \log_2 K \rceil$ qubits. Note that, even though the coherent states $|\pm\alpha\rangle = \sum_{n=0}^{\infty} e^{-|\alpha|^2/2} (|\pm\alpha\rangle^n / \sqrt{n!}) |n\rangle$ are embedded in an infinite dimensional space spanned by the photon number (Fock) states $\{|n\rangle\}$, since the hypothesis states span a finite dimensional space, the entire relevant information can be *compressed* down to a finite dimensional space, e.g., the state of a collection of qubits. Helstrom showed that minimum-error discrimination of K linearly independent pure states in \mathcal{A} requires a K -outcome projective measurement in the span of \mathcal{A} [1]. Thus, assuming $U_{\mathcal{A}}$ can be implemented to compress the hypothesis states to one of K states of $\lceil \log_2 K \rceil$ qubits, Helstrom's optimal projective measurement can be implemented by a unitary rotation on the compressed state, followed by measurement of the qubits. However, it is not at all obvious how to implement $U_{\mathcal{A}}$ in the coherent-state case, as it corresponds to a highly nonlinear optical transformation. This is where, our second observation—a unique property of coherent states—comes in handy.

The second observation is that a coherent state $|\alpha_j\rangle$ can be *sliced* into n independent coherent states of smaller amplitudes

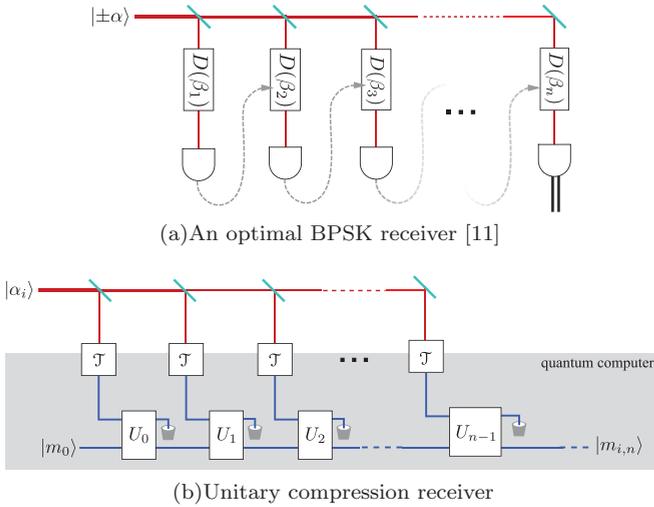


FIG. 1. (Color online) (a) It is possible to distinguish between two coherent states (red lines) optimally by “slicing” the input state and measuring each slice adaptively—the outcome of each photon detection measurement (gray dashed arrows) being used to perform a displacement on the input of the next measurement. Once the final slice is measured, the final outcome (double solid line) is used to make a decision about which hypothesis was more likely to have been received. This is the class of receivers shown in Ref. [5] to be optimal for binary hypotheses. (b) Here we demonstrate that, instead of measuring each slice adaptively, one can transfer (\mathcal{T}) each coherent slice into a quantum computer (shaded region), and the information in the qubits (blue lines) can be efficiently and coherently *compressed* by the unitaries U_ℓ into a small ancilla quantum register [12], so that the final state $|m_{i,n}\rangle$ of the register can then be measured or processed further as part of a multimode receiver as discussed in the text. This unitary compression receiver can be customized to any set of coherent-state hypotheses, and its design is independent of the figure of merit being optimized, as all information about the received state is compressed into the final state of the ancilla register.

using a $1:n$ symmetric beamsplitter, i.e., $|\alpha_j\rangle \rightarrow |\beta_j\rangle \otimes |\beta_j\rangle \otimes \dots \otimes |\beta_j\rangle$, for $\beta_j = \alpha_j/\sqrt{n}$. Furthermore, for n large, $|\beta_j| \ll 1$ which implies the average photon number in the slices is small, and we find $|\beta_j\rangle \approx \frac{|0\rangle + \beta_j|1\rangle}{\sqrt{1+|\beta_j|^2}} \equiv |h_j\rangle$. In other words, any coherent state can be split into multiple copies of weak coherent states, each of which can be faithfully represented by a qubit encoded in the vacuum $|0\rangle$ and single photon $|1\rangle$ states (also known as a *single-rail qubit encoding* [11]).

It is now easy to see how to explicitly construct U_A by concatenating n unitary gates. We start with a $\lceil \log_2 K \rceil$ -qubit ancilla register prepared in some initial state $|m_0\rangle$. We then unitarily compress the received state $|\alpha_j\rangle$, one slice $|\alpha_j/\sqrt{n}\rangle$ at a time, into the state of the register, following the proposal by Blume-Kohout *et al.* for the general multicopy quantum hypothesis test [12]. This is done using a sequence of $(1 + \lceil \log_2 K \rceil)$ -qubit entangling gates U_ℓ acting jointly on the ℓ th slice and the ancilla register, eventually transforming the ancilla register to a state $|m_{j,n}\rangle$. More precisely, we require

$$U_\ell |h_j\rangle |m_{j,\ell}\rangle = |\phi\rangle |m_{j,\ell+1}\rangle, \quad (1)$$

for all hypothesis states $|h_j\rangle$, where $|\phi\rangle$ is a fixed quantum state independent of the hypothesis i which can then be discarded as it contains no relevant information.

It is possible to do this state transfer in such a way that the Gram matrix elements of the compressed ensemble approach the Gram matrix of the original coherent-state ensemble, i.e., $\gamma_{jk}^{(n)} \equiv \langle m_{j,n} | m_{k,n} \rangle \rightarrow \gamma_{jk}$, in the limit of many slices ($n \rightarrow \infty$). This follows from the fact that the collection of qubit states approximating the slices of coherent states have inner products arbitrarily close to the overlap of the original coherent states in the limit of large n , i.e., $\lim_{n \rightarrow \infty} \langle h_j | h_k \rangle^n = \langle \alpha_j | \alpha_k \rangle$. As we discuss above, once the coherent-state ensemble \mathcal{A} has been compressed faithfully into the ancilla register, any additional quantum processing can be performed without any loss in performance. For the purposes of minimum-error discrimination between the hypothesis states, a projective measurement of the ancilla states is required. This can be implemented by a unitary rotation U_H on the register’s state followed by a computational-basis measurement. Since the number of gates necessary to implement an arbitrary N -qubit unitary is exponential in N [13], the number of gates necessary to build U_H is only polynomial in the number of hypotheses K . Therefore, the receiver is efficient from the resource-scaling point of view. Moreover, computing U_H requires solving a set of K^2 nonlinear simultaneous equations prescribed by Helstrom [1], which can be done with an overhead that is polynomial in K . See Fig. 1(b) for an illustration of the compression unitaries acting sequentially on n slices of the received state.

Finally, unlike Dolinar’s optimal binary-discrimination receiver—which adaptively, albeit *destructively*, measures tiny slices of the received coherent state—our receiver coherently couples slices of the received coherent state into a $\lceil \log_2 K \rceil$ dimensional quantum register, the final state of which has the entirety of the relevant quantum information that was present in the original coherent state. The adaptive destructive measurement strategy corresponds to a local operations and classical communication (LOCC) strategy. If our final measurement is written in terms of its action on the slices, it becomes clear that our approach amounts to a collective quantum measurement, thereby sidestepping the LOCC limitations of the generalized Dolinar strategy.

A. Binary discrimination

As an illustration, consider the compression unitaries for distinguishing between the equi-prior binary phase-shift keying (BPSK) ensemble of coherent states $|\pm\alpha\rangle$, where $\alpha \in \mathbb{R}$. Any pair of coherent states can be transformed to this ensemble via simple linear-optical transformations. Although the Dolinar receiver can distinguish these states with the quantum-limited minimum probability of error, the compression approach is more flexible, as it is possible to perform additional quantum processing of the compressed state in the ancilla register, enabling multimode applications, as is discussed later. Moreover, the construction of the minimum-error-discrimination receiver for the binary case generalizes straightforwardly to larger sets of hypotheses.

After slicing via a symmetric $1:n$ beamsplitter, the hypothesis states can be approximated well by the states $|h_j\rangle^{\otimes n} = \left(\frac{|0\rangle + \beta_j|1\rangle}{\sqrt{1+|\beta_j|^2}}\right)^{\otimes n}$, where $\beta_{\pm 1} = \pm\alpha/\sqrt{n}$. We assume that n is chosen large enough such that $|\beta_j| \ll 1$ holds. Since $K = 2$,

only one ancilla qubit is required. Let us denote the input state of the ancilla qubit for the ℓ th compression step under hypothesis j as $|m_{j,\ell}\rangle$ [see Fig. 1(b)], the initial state of the ancilla $|m_{j,0}\rangle = |0\rangle$, and the ℓ th compression unitary, U_ℓ . The 0th compression step is to map $|h_j\rangle|m_{j,0}\rangle$ to $|0\rangle|m_{j,1}\rangle$, and a natural choice to make is $|m_{j,1}\rangle = |h_j\rangle$, so that U_0 is just the exchange of the input and the ancilla states—the well-known two-qubit swap gate.

The subsequent compression operations have to satisfy

$$U_\ell|h_{-1}\rangle|m_{-1,\ell}\rangle = |0\rangle|m_{-1,\ell+1}\rangle, \quad (2)$$

$$U_\ell|h_{+1}\rangle|m_{+1,\ell}\rangle = |0\rangle|m_{+1,\ell+1}\rangle, \quad (3)$$

i.e., all the information about the received slices is compressed, sequentially, into the ancilla qubit. We choose $|m_{j,\ell}\rangle$ to be of the same general form as $|h_j\rangle$ but with different parameters. In particular, we can choose $|m_{j,\ell}\rangle = \frac{|0\rangle + jB_{(\ell)}|1\rangle}{\sqrt{1+B_{(\ell)}^2}}$, for some $B_{(\ell)}$, and given the fact that U_ℓ preserves the inner product, we obtain the recursion relation $B_{(\ell+1)} = \sqrt{\frac{\alpha^2/n+B_{(\ell)}^2}{1+\alpha^2B_{(\ell)}^2/n}}$ and $B_{(0)} = 0$.

The recursion relation for $B_{(\ell)}$ can be solved by using standard methods, yielding

$$B_{(\ell)} = \sqrt{1 + \frac{2}{(-1)^\ell \left(\frac{\beta^2+1}{\beta^2-1}\right)^{\ell+1} - 1}}, \quad (4)$$

where $\ell > 0$ and β is the amplitude of the hypothesis slices.

Given this parameter and the constraint (2) and (3), the relevant two-dimensional block of U_ℓ is uniquely determined. For our purposes, the remaining block can be chosen arbitrarily to complete the unitary, e.g., resulting in

$$U_{\ell>0} = \begin{bmatrix} \frac{1}{\sqrt{1+\beta^2B_{(\ell)}^2}} & 0 & 0 & \frac{\beta B_{(\ell)}}{\sqrt{1+\beta^2B_{(\ell)}^2}} \\ 0 & \frac{B_{(\ell)}}{\sqrt{\beta^2+B_{(\ell)}^2}} & \frac{\beta}{\sqrt{\beta^2+B_{(\ell)}^2}} & 0 \\ 0 & \frac{\beta}{\sqrt{\beta^2+B_{(\ell)}^2}} & -\frac{B_{(\ell)}}{\sqrt{\beta^2+B_{(\ell)}^2}} & 0 \\ \frac{\beta B_{(\ell)}}{\sqrt{1+\beta^2B_{(\ell)}^2}} & 0 & 0 & -\frac{1}{\sqrt{1+\beta^2B_{(\ell)}^2}} \end{bmatrix}. \quad (5)$$

Finally, the inner product between compressed ancilla states for the hypothesis states $|h_j\rangle = \frac{|0\rangle + j\frac{\alpha}{\sqrt{n}}|1\rangle}{\sqrt{1+\frac{\alpha^2}{n}}}$ is given by

$$\left(\frac{1 - \frac{\alpha^2}{n}}{1 + \frac{\alpha^2}{n}}\right)^{n+1}, \quad (6)$$

which in the limit of $n \rightarrow \infty$ reduces to $\langle -\alpha|\alpha\rangle = e^{-2\alpha^2}$ as claimed.

It can be easily shown that the measurement that distinguishes the final compressed hypotheses $|m_{i,n-1}\rangle$ with minimum-error probability is a measurement in the basis $|0\rangle \pm |1\rangle$. The error probability is given by $(1 - B_{(n)})^2/2(1 + B_{(n)}^2)$, which in the limit of $n \rightarrow \infty$ equals the Helstrom bound $(1 - \sqrt{1 - e^{-4\alpha^2}})/2$, demonstrating that performance can approximate the optimal value for any α arbitrarily well.

III. LOSS AND TRANSFER OF OPTICAL STATES TO QUBITS

In the presence of photon loss during the slicing of the coherent-state hypotheses, the states $|\beta_j\rangle$ are mapped to $|\beta_j\sqrt{1-\eta}\rangle$, where η is the overall photon loss probability. For known η , this loss can be accounted for to reach the Helstrom bound for the scaled hypotheses $|\alpha_j\sqrt{1-\eta}\rangle$ instead. Just as in the optimal proposals for the binary case [2,5], this degradation cannot be avoided, but in well-engineered systems η is expected to be $<10^{-2}$ and therefore not significant.

As described above, the ability to implement a universal set of qubit operations is essential for the implementation of our proposal for quantum-limited minimum-error discrimination of coherent-state signals. However, operations on single-rail qubits suffer from significant technical challenges [11]. Viable optical implementations of general deterministic single-qubit operations remain unknown, and two-qubit interactions are also challenging.

This problem can be avoided by transferring the optical state of the slices into another qubit realization where such operations are more easily implemented. We consider two possibilities: (a) the ideal mapping of the $\{|0\rangle, |1\rangle\}$ subspace of the optical mode to a qubit, and (b) a stimulated Raman adiabatic passage (STIRAP) based transfer of the optical mode state to an atomlike system that can then be manipulated as a qubit [14]. In both cases we take the unitary manipulation of the resulting states to be unrestricted and consider only the degradation effects of the transfer process (noise in the quantum computer can be handled using standard fault-tolerance techniques [15]). As the sections that follow illustrate, the result is that, instead of having each slice of the coherent state map to the pure states $|h_j\rangle$, one obtains the mixed states $\rho_{\beta_j}^{(a)} = e^{-\beta_j^2}|h_j\rangle\langle h_j| + (1 - e^{-\beta_j^2})|0\rangle\langle 0|$ and $\rho_{\beta_j}^{(b)} = e^{-\beta_j^2}|h_j\rangle\langle h_j| + (1 - e^{-\beta_j^2})|1\rangle\langle 1|$, corresponding to the two possibilities for the transfer procedure described above, and which deviate from the qubit hypotheses due to populations in the subspace with two photons or more. Despite this source of decoherence, it is always possible to make the distinguishability between the collection of transferred states and the collection of corresponding pure-state hypotheses arbitrarily small by making n sufficiently large (see Secs. III A and III B). This translates to being able to use the unitaries U_ℓ designed for the pure states $|h_j\rangle$ on the mixed states $\rho_{\beta_j}^{(a)}$ and $\rho_{\beta_j}^{(b)}$, while remaining arbitrarily close to the Helstrom bound for the minimum probability of error, as illustrated in Fig. 2.

A. Ideal unitary transfer of 0/1 photon subspace to qubits

Given any quantum state of an optical mode decomposed in the basis of Fock states (or photon number states) $|n\rangle_F$ for $n \geq 0$, it is in principle possible to unitarily swap the contents of the $|0\rangle_F/|1\rangle_F$ subspace with a qubit. The unitary that performs this operation is

$$\begin{aligned} &|0\rangle\langle 0|_F \otimes |0\rangle\langle 0| + |1\rangle\langle 1|_F \otimes |1\rangle\langle 1| + |0\rangle\langle 1|_F \otimes |1\rangle\langle 0| \\ &+ |1\rangle\langle 0|_F \otimes |0\rangle\langle 1|, \end{aligned} \quad (7)$$

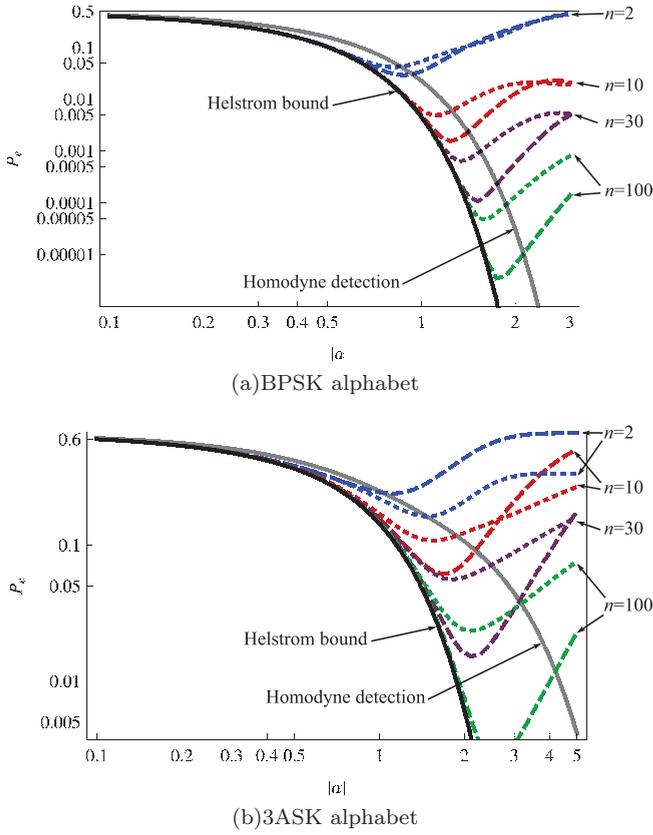


FIG. 2. (Color online) The minimum-error probability of distinguishing between a set of coherent states as a function of the amplitude α follows the well-known bound given by Helstrom [1] (solid black curves). Maximum-likelihood estimation of the hypothesis based on homodyne detection leads to higher error rates (solid gray curves). The receiver described here has a probability of error arbitrarily close to the minimum for sufficiently small α/\sqrt{n} . This is illustrated by the curves for ideal unitary transfer (dashed) and STIRAP state transfer (dotted), both in the (a) binary alphabet case and in the (b) ternary alphabet case, for $n = 2$ (blue), $n = 10$ (red), $n = 30$ (purple), and $n = 100$ (green) slices.

and by applying this operation to the state $|\beta_j\rangle|0\rangle$ and tracing out the optical mode, one obtains

$$\rho_{\beta_j}^{(a)} = e^{-\beta_j^2} |h_j\rangle\langle h_j| + (1 - e^{-\beta_j^2}) |0\rangle\langle 0|, \quad (8)$$

so the fidelity to $|h_j\rangle$ is given by

$$F^{(a)}(\beta_j) = e^{-|\beta_j|^2} |\beta_j|^2 + \frac{1}{1 + |\beta_j|^2}. \quad (9)$$

One finds

$$F^{(a)}(\alpha/\sqrt{n})^n = 1 - \frac{|\alpha|^6}{2n^2} + O\left(\frac{|\alpha|^8}{n^3}\right), \quad (10)$$

so that even by manipulating only the 0/1 photon subspace and ignoring the higher excitations, the collection of transferred states can be made arbitrarily close to the collection of ideal slices of any hypothesis.

B. STIRAP transfer of 0/1 photon subspace to qubits

The transfer of the photonic excitation into a cavity mode enables the use of STIRAP to coherently exchange a single excitation between the cavity mode and a qubit. The unitary that corresponds to this operation is

$$\sum_{n=1}^{\infty} |n-1\rangle\langle n|_F \otimes |1\rangle\langle 0| + \sum_{n=1}^{\infty} |n\rangle\langle n-1|_F \otimes |0\rangle\langle 1| + |0\rangle\langle 0|_F \otimes |0\rangle\langle 0|, \quad (11)$$

and by applying this operation to the state $|\beta_j\rangle|0\rangle$ and tracing out the optical mode, one obtains

$$\rho_{\beta_j}^{(b)} = e^{-\beta_j^2} |h_j\rangle\langle h_j| + (1 - e^{-\beta_j^2}) |1\rangle\langle 1|, \quad (12)$$

so the fidelity to $|h_j\rangle$ is given by

$$F^{(b)}(\beta_j) = e^{-|\beta_j|^2} + \frac{|\beta_j|^2}{1 + |\beta_j|^2}. \quad (13)$$

One finds a similar series expansion for the sliced case,

$$F^{(b)}(\alpha/\sqrt{n})^n = 1 - \frac{|\alpha|^4}{2n} + O\left(\frac{|\alpha|^6}{n^2}\right), \quad (14)$$

so that just as in the ideal unitary transfer case, the collection of transferred states can be made arbitrarily close to the collection of ideal slices of any hypothesis.

Similar performance can also be obtained via a tunable Jaynes-Cummings interaction between a cavity mode and a qubitlike system.

IV. TERNARY AND MULTIMODE CASES

Let us consider now the case of three coherent-state hypotheses, which for simplicity we take to be $|j\alpha\rangle$ for $j \in \{-1, 0, 1\}$ (i.e., a displaced ternary amplitude-shift keying or 3ASK alphabet, where the displacement adds symmetry to simplify the analysis). No known generalization of the optimal receivers for BPSK can achieve the minimum probability of error in distinguishing these three states, but our coherent compression receiver can. Using the same approach of slicing the coherent states to obtain states that are well approximated by qubit states, we simply need to specify the unitaries V_ℓ that perform the compression. In this case, we choose the ancilla states to have the form

$$|m'_{j,\ell}\rangle = \frac{|00\rangle + jC_{(\ell)}|01\rangle + j^2D_{(\ell)}|11\rangle}{\sqrt{1 + j^2C_{(\ell)}^2 + j^2D_{(\ell)}^2}}, \quad (15)$$

with the resulting coupled recursion relations given by

$$C_{(\ell+1)} = \frac{\alpha}{\sqrt{n}} \sqrt{C_{(\ell)}^2 + \alpha^2/n + \alpha^2 D_{(\ell)}^2/n}, \quad (16)$$

$$D_{(\ell+1)} = \sqrt{D_{(\ell)}^2 + \alpha^2 C_{(\ell)}^2/n}, \quad (17)$$

$$C_{(0)} = D_{(0)} = 0, \quad (18)$$

which, as in the binary case, can be solved exactly.

The constraints for the compression unitary V_ℓ have a similar form as in the BPSK case constraints (2) and (3), although now there are three hypotheses, resulting in

$$V_\ell |h'_{-1}\rangle |m'_{-1,\ell}\rangle = |0\rangle |m'_{-1,\ell+1}\rangle, \quad (19)$$

$$V_\ell |h'_0\rangle |m'_{0,\ell}\rangle = |0\rangle |m'_{0,\ell+1}\rangle, \quad (20)$$

$$V_\ell |h'_{+1}\rangle |m'_{+1,\ell}\rangle = |0\rangle |m'_{+1,\ell+1}\rangle, \quad (21)$$

while the remaining degrees of freedom of V_ℓ can be completed arbitrarily for our purposes. This results in

$$V_{\ell>0} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{C_{(\ell)}}{\sqrt{\beta^2 + C_{(\ell)}^2 + \beta^2 D_{(\ell)}^2}} & 0 & 0 & \frac{\beta}{\sqrt{\beta^2 + C_{(\ell)}^2 + \beta^2 D_{(\ell)}^2}} & 0 & 0 & \frac{\beta D_{(\ell)}}{\sqrt{\beta^2 + C_{(\ell)}^2 + \beta^2 D_{(\ell)}^2}} \\ 0 & * & * & * & * & * & * & * \\ 0 & 0 & \frac{D_{(\ell)}}{\sqrt{D_{(\ell)}^2 + \beta^2 C_{(\ell)}^2}} & 0 & \frac{\beta C_{(\ell)}}{\sqrt{D_{(\ell)}^2 + \beta^2 C_{(\ell)}^2}} & 0 & 0 & 0 \\ 0 & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * \end{bmatrix}, \quad (22)$$

where once again the * entries are free parameters.

The recurrence relation for $C_{(\ell)}$ and $D_{(\ell)}$ can also be solved analytically, yielding

$$C_{(\ell)} = \sqrt{\frac{(1 + \beta^2)^\ell - (1 - \beta^2)^\ell}{2}}, \quad (23)$$

$$D_{(\ell)} = \sqrt{\frac{(1 + \beta^2)^\ell + (1 - \beta^2)^\ell}{2}} - 1, \quad (24)$$

where $\ell > 0$ and β is the amplitude of the hypothesis slices.

The Gram matrix (the matrix of inner products) for the three compressed hypothesis states is

$$\begin{bmatrix} 1 & \left(\frac{n}{n+\alpha^2}\right)^{n/2} & \left(\frac{n}{n+\alpha^2}\right)^{n/2} \\ \left(\frac{n}{n+\alpha^2}\right)^{n/2} & 1 & \left(\frac{n-\alpha^2}{n+\alpha^2}\right)^n \\ \left(\frac{n}{n+\alpha^2}\right)^{n/2} & \left(\frac{n-\alpha^2}{n+\alpha^2}\right)^n & 1 \end{bmatrix}, \quad (25)$$

which reduces to the Gram matrix for the three coherent-state hypotheses in the 3ASK alphabet in the limit of $n \rightarrow \infty$ as claimed.

For a finite number of slices n , the minimum-error probability for distinguishing the states in the 3ASK alphabet can be computed semianalytically (see the Appendix), and the same general behavior of the BPSK case, where the performance approaches the Helstrom limit, can be observed for the 3ASK case as well, as illustrated in Fig. 2(b).

This compression receiver approach opens the door to quantum-limited optimization of metrics other than the probability of error in detection of a coherent-state ensemble. Examples are maximizing the one-shot accessible information of an ensemble for the optimal measurement choice [16] and minimizing the phase-space Euclidean norm in detecting a coherent state from a constellation. This is because the

compression operations are independent of how the final measurement of the ancilla register is optimized.

Another notable feature of this general class of receivers, as alluded to earlier, is the possibility of additional quantum processing of the compressed states. This enables, in particular, the discrimination of multimode coherent states (such as the ones used in sensing or coded communications applications) by reusing the compression operations for single-mode states. For example, if one would like to discriminate between the three states, $|+\alpha\rangle|+\alpha\rangle|-\alpha\rangle|-\alpha\rangle$, $|-\alpha\rangle|+\alpha\rangle|+\alpha\rangle|-\alpha\rangle$, and $|-\alpha\rangle|-\alpha\rangle|+\alpha\rangle|+\alpha\rangle$, one would slice and compress the state of each mode independently using our coherent BPSK receiver, but instead of measuring the four compressed ancilla states corresponding to each mode, one would perform additional compression of these states into a three-dimensional subspace of a two-qubit register. The coherent compression ensures that the Helstrom bound for distinguishing between the three states can be reached, while the individual measurement of each mode leads to a higher error probability.

This modularity also allows for a systematic way to develop receivers that surpass the Shannon capacity of an optical channel with structured optical receivers and to approach the Holevo limit to the rate at which classical data can be sent reliably over an optical channel [9,16]. This can be done by first compressing each of the N code-word symbols—which are coherent states from a known and finite M -ary constellation—into the states of N separate $\lceil \log_2 M \rceil$ -qubit registers. These states are then unitarily transformed in such a way that the naturally accessible measurements in the system correspond to the optimal measurements for minimum-error discrimination of the code-word states. One may be able to find efficient implementations of this unitary transformation by leveraging the structure of Holevo-capacity-achieving error-correcting codes [17].

V. SUMMARY

We have demonstrated how to construct a receiver to discriminate between any set of coherent-state (laser light) signals, using a small special-purpose quantum computer. Our solution leverages two properties of coherent states of light—first, that splitting a coherent state via a beamsplitter produces independent coherent states with smaller amplitudes, and second, that a coherent state of a small amplitude is well approximated by a qubit encoded by the vacuum and the one-photon Fock state of an optical mode, the single-rail qubit. These two properties, in conjunction with a recent result on distinguishing multicopy quantum hypotheses by a sequential coherent-processing receiver [12], leads to an explicit construction of an optimal receiver for any specified coherent-state hypothesis test. This solves the long-standing problem of building receivers that can achieve the Helstrom limit for nonbinary coherent-state signals. There remain practical challenges in implementing our receiver because universal quantum computing on single-rail qubits still eludes us. However, we address one potentially practical means to implement our receiver by transferring the state of an optical mode to an atomic system [14]. Our solution also opens the door to the quantum-limited optimization of other important metrics, such as achieving the Holevo bound on the rate of classical information transmission over a quantum channel. This would allow for reliable information transmission on an optical channel at rates higher than the Shannon limit of any known receiver.

ACKNOWLEDGMENTS

The authors thank Mark Wilde for pointing Ref. [12] out to us and for useful discussions. This research was supported by the DARPA Information in a Photon (InPho) program under Contract No. HR0011-10-C-0162.

APPENDIX: MINIMAL PROBABILITY OF ERROR MEASUREMENT FOR THREE HYPOTHESES WITH ISOSCELES CONFIGURATION

Here we briefly describe a minor generalization of an example from Helstrom's book [1] so that it can be applied to the minimal error probability discrimination of both coherent states and qubit hypothesis states (details of the derivation can be found in Ref. [1]).

Consider three linearly independent pure-state hypotheses with corresponding Gram matrix

$$\Gamma = \begin{bmatrix} 1 & x & x \\ x & 1 & y \\ x & y & 1 \end{bmatrix}, \quad (\text{A1})$$

where, in our case, $x = \langle 0|\alpha\rangle$ and $y = \langle -\alpha|\alpha\rangle$, but this need not be the case in general. Due to the symmetry of the Gram matrix, the matrix Ξ of the inner products $\langle w_i|\psi_j\rangle$ between the optimal projectors $|w_i\rangle$ and the hypotheses $|\psi_j\rangle$ is restricted to take the form

$$\Xi = \begin{bmatrix} a & d & d \\ d & c & e \\ d & e & c \end{bmatrix}, \quad (\text{A2})$$

where the matrix elements must satisfy the following constraints [1]:

$$a^2 + 2b^2 = 1, \quad (\text{A3})$$

$$d^2 + c^2 + e^2 = 1, \quad (\text{A4})$$

$$ad + b(c + e) = x, \quad (\text{A5})$$

$$d^2 + 2ce = y, \quad (\text{A6})$$

$$ab = cd. \quad (\text{A7})$$

Solving the first four constraints in terms of d results in

$$a = \frac{2dx + \sqrt{(y - 2x^2 + 1)(y - 2d^2 + 1)}}{1 + y}, \quad (\text{A8})$$

$$b = \frac{x - 2d^2x + xy - d\sqrt{(y - 2x^2 + 1)(y - 2d^2 + 1)}}{(1 + y)\sqrt{y - 2d^2 + 1}}, \quad (\text{A9})$$

$$c = \frac{1}{2}(\sqrt{y - 2d^2 + 1} + \sqrt{1 - y}), \quad (\text{A10})$$

$$e = \frac{1}{2}(\sqrt{y - 2d^2 + 1} - \sqrt{1 - y}), \quad (\text{A11})$$

which can then be plugged into the fifth constraint to solve for d numerically. The resulting Ξ matrix describes the optimal projectors to discriminate between the hypotheses described by the Gram matrix Γ with a minimal probability of error of $1 - \frac{1}{3}(a^2 + 2c^2)$.

-
- [1] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
- [2] S. J. Dolinar, Research Laboratory of Electronics, MIT Technical Report No. 111, 1973.
- [3] R. S. Kennedy, Research Laboratory of Electronics, MIT Technical Report No. 110, 1972.
- [4] R. L. Cook, P. J. Martin, and J. M. Geremia, *Nature (London)* **446**, 774 (2007).
- [5] M. Takeoka, M. Sasaki, and Norbert Lütkenhaus, *Phys. Rev. Lett.* **97**, 040502 (2006).
- [6] S. J. Dolinar, Jr., Telecommunications and Data Acquisition Progress Report 42-72, 1983, pp. 30-42.
- [7] R. S. Bondurant, *Opt. Lett.* **18**, 1896 (1993).
- [8] J. Chen, J. L. Habif, Z. Dutton, R. Lazarus, and S. Guha, *Nat. Photonics* **6**, 374 (2012).
- [9] S. Guha, *Phys. Rev. Lett.* **106**, 240502 (2011).
- [10] H.-W. Chung, S. Guha, and L. Zheng, in *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, St. Petersburg, 2011), pp. 284-288.

- [11] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).
- [12] R. Blume-Kohout, S. Croke, and M. Zwolak, arXiv:1201.6625.
- [13] A. Yu. Kitaev, *Russ. Math. Surv.* **52**, 1191 (1997).
- [14] D. K. L. Oi, V. Potocek, and J. Jeffers, arXiv:1207.3011.
- [15] P. Aliferis, D. Gottesman, and J. Preskill, *Quantum Inf. Comput.* **6**, 97 (2006).
- [16] A. S. Holevo, *Teoret. Mat. Fiz.* **17**, 319 (1973).
- [17] S. Guha and M. Wilde, in *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, Cambridge, 2012), pp. 546–550.