Polar coding to achieve the Holevo capacity of a pure-loss optical channel

Saikat Guha
Disruptive Information Proc. Tech. Group
Raytheon BBN Technologies
Cambridge, Massachusetts, USA 02138

Mark M. Wilde
School of Computer Science
McGill University
Montreal, Québec, Canada H3A 2A7

***Abstract*—In the low-energy high-energy-efficiency regime of classical optical communications—relevant to deep-space optical channels—there is a big gap between reliable communication rates achievable via conventional optical receivers and the ultimate (Holevo) capacity. Achieving the Holevo capacity requires not only optimal codes but also receivers that make collective measurements on long (modulated) codeword waveforms, and it is impossible to implement these collective measurements via symbol-by-symbol detection along with classical postprocessing [1], [2]. Here, we apply our recent results on the *classical-quantum polar code* [3]—the first near-explicit, linear, symmetric-Holevo-rate achieving code—to the lossy optical channel, and we show that it almost closes the entire gap to the Holevo capacity in the low photon number regime. In contrast, Arikan's original polar codes, applied to the DMC induced by the physical optical channel paired with any conceivable structured optical receiver (including optical homodyne, heterodyne, or direct-detection) fails to achieve the ultimate Holevo limit to channel capacity. However, our polar code construction (which uses the quantum fidelity as a channel parameter rather than the classical Bhattacharyya quantity to choose the "good channels" in the polar-code construction), paired with a quantum successive-cancellation receiver—which involves a sequence of collective non-destructive binary projective measurements on the joint quantum state of the received codeword waveform—can attain the Holevo limit, and can hence in principle achieve higher rates than Arikan's polar code and decoder directly applied to the optical channel. However, even a theoretical recipe for construction of an optical realization of the quantum successive-cancellation receiver remains an open question.**

Determining the ultimate limits on optical communication must involve an explicitly quantum analysis, because electromagnetic waves are fundamentally quantum mechanical and high-sensitivity photodetection systems are limited by noise of quantum-mechanical origin. In quantum mechanics, the state of a physical system together with a description of the measurement made on that system determine the statistics of the measurement outcomes. Thus, in seeking the classical information capacity of an optical channel, we must allow for optimization over *both* the transmitted quantum states *and* the receiver's quantum measurement. In particular, it seems inappropriate to restrict consideration to coherent-state (laser) transmitters and coherent-detection or direct-detection receivers. Imposing these structural constraints leads to Gaussian-noise (Shannon-type) capacity formulas for coherent (homodyne and heterodyne) detection and Poisson-noise capacity results for shot-noise-limited direct detection [4], [5]. None of these results, however, can be regarded as specifying the ultimate limit on reliable communication at optical frequencies. What is needed for deducing the fundamental limits on optical communication is an analog of Shannon's channel coding theorem—but free of unjustified structural constraints on the transmitter and receiver—that applies to data transmission over a *quantum channel*, viz., the Holevo-Schumacher-Westmoreland (HSW) theorem [6], [7], [8].

The HSW theorem, along with the Yuen-Ozawa converse [8], specifies the channel capacity of a pure-loss optical channel [1]. Even though the single-letter Holevo quantity is an achievable rate, the receiver in general must make joint-detection (*collective*) measurements over long codeword blocks—measurements that cannot be realized by detecting single-modulation symbols followed by classical decoding. For the pure-loss optical channel, a coherent-state modulation suffices to attain the ultimate capacity, i.e., use of non-classical transmitted states or entangled codewords does not increase capacity [1]. We will use the term *Holevo capacity* unambiguously in this paper to refer to the single-letter Holevo rate of the pure-loss optical channel. The square-root-measurement, which in general is a positive operator-valued measure (POVM), applied to a random code gives the mathematical construct of a receiver measurement that can achieve the Holevo capacity [7]. The key questions that remain are how to design practical modulation formats, explicit codes (with efficient encoders), and most importantly, structured laboratory-realizable designs of Holevo-capacity-achieving joint-detection receivers (JDRs).

Lloyd *et al.* [9] conceptualized a receiver that can attain the Holevo capacity of any quantum channel by making a sequence of "yes/no" projective measurements on codewords of a random codebook. However, the translation of their strategy to a structured receiver design for the optical channel was not clear. Sen later simplified Lloyd *et al.*'s proof [10], and after this, we showed how to apply Sen's result in order to achieve the Holevo capacity of the pure-loss optical channel [11]. The strategy employs a random code and a sequence of multi-mode phase-space displacements and quantum-non-demolition "vacuum-or-not" measurements. In Ref. [2], one of us showed

SG was supported by the DARPA Information in a Photon (InPho) program under DARPA/CMO Contract No. HR0011-10-C-0159. 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 U.S. Government. MMW acknowledges financial support from Centre de Recherches Mathématiques.

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

some of the first examples of structured optical JDRs for BPSK modulated binary codes, which induce superchannels over a codebook whose Shannon capacity per symbol is higher than the Shannon capacity of the single-use DMC induced by an optimal measurement on each received BPSK symbol [12]. In recent work, we generalized Arikan's *polar code* for the classical channel, to the *classical-quantum* (cq) polar code that can achieve the symmetric Holevo information for sending classical information over any quantum channel, i.e., the Holevo information rate when the input symbols are assigned equal priors [3]. This was the first explicit (and linear) code that provably achieves the Holevo capacity, and a careful inspection of [3] reveals that this extension was non-trivial.

In this paper, we bring together our works from Refs. [2], [3] to show that a cq-polar code essentially achieves the Holevo capacity of the optical channel with BPSK modulation. We show that at low mean pulse energy (photon number), this capacity is extremely close to the ultimate Holevo capacity (that with an unrestricted modulation). The receiver for our polar code is a quantum-limited successive-cancellation (SC) JDR that detects and decodes successively, while acting on the entire N-BPSK-symbol optical codeword waveform. It performs NR binary-outcome, quantum-non-demolition measurements (as opposed to the 2^{NR} measurement stages in [9], [11]), decoding one message bit at a time. The final piece of the puzzle, a structured optical receiver design that implements our quantum SC decoder, remains a subject of ongoing research.

I. Capacity of the pure-loss optical channel

Consider a lossy optical channel with transmissivity $\eta \in (0,1]$. Each channel use is a T-sec-long pulse slot that can transmit one modulation symbol. The mean energy[1] per transmitted pulse is constrained to E photons per channel use. The Holevo capacity of this channel is given by $g(\eta E)$ bits/use, where $g(x) = (1+x)\log(1+x) - x\log x$. A $\sqrt{\text{photons/sec}}$-unit laser pulse $s(t)e^{j(\omega_0+\theta)t}, t \in [0,T)$ has energy $E_s = \int_0^T |s(t)|^2 dt$ photons. Quantum-mechanically, the state of this pulse is a coherent state $|\alpha\rangle$, with $\alpha = \sqrt{E_s}e^{j\theta}$, where θ is taken w.r.t. some carrier-phase reference.[2] Since the channel preserves coherent states (with amplitude attenuation), $|\alpha\rangle \to |\sqrt{\eta}\alpha\rangle$, let us assume WLOG that $\eta = 1$ (or, equivalently, treat E as the average received energy per pulse). The capacity-achieving input distribution is the isotropic Gaussian distribution $p(\alpha) = e^{-|\alpha|^2/E}/\pi E$, and the ultimate Holevo capacity, $C_{\text{ult}}(E) = g(E)$ bits/symbol.

Let us consider an equi-prior (received) BPSK alphabet $\left\{|\sqrt{E}\rangle, |-\sqrt{E}\rangle\right\}$. The minimum average probability of error in discriminating the two BPSK pulses is given by $P_{e,\min} = \left[1-\sqrt{1-e^{-4E}}\right]/2$, which can be attained exactly by the *Dolinar receiver* [12]. An ideal homodyne receiver achieves $P_{e,\text{hom}} = \text{erfc}\left(\sqrt{2E}\right)/2$. Using either the Dolinar receiver or the homodyne receiver on the BPSK pulses induces a binary symmetric channel (BSC) with crossover probabilities $P_{e,\min}$ and $P_{e,\text{hom}}$, thus attaining channel capacities,[3] $C_1(E) = 1 - H_2(P_{e,\min})$ and $C_{\text{hom}}(E) = 1 - H_2(P_{e,\text{hom}})$ bits/symbol, respectively, where $H_2(\cdot)$ is the binary entropy function. Another strategy is to use the Kennedy receiver, which coherently shifts the BPSK constellation to $\left\{|2\sqrt{E}\rangle, |\sqrt{0}\rangle\right\}$, followed by direct detection (Poisson statistics). This induces a Z-channel with crossover probability e^{-4E} and with $P_{e,\text{Ken}} = e^{-4E}/2$.

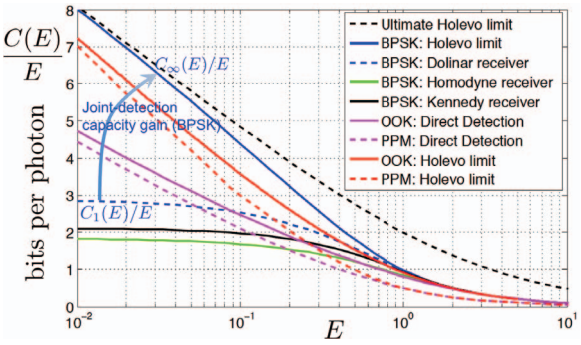

Fig. 1. Energy efficiency (bits/photon) vs. the mean pulse energy E. The arrow indicates the performance gap between Arikan's polar code paired with a classical decoder applied to the optical channel and our classical-quantum polar code paired with a quantum decoder.

Consider a binary pure-state channel of the form $W : x \to |\psi_x\rangle$, where W denotes the channel, $x \in \{0,1\}$, and $|\psi_x\rangle$ are pure-state channel outputs. For the BPSK channel, $|\psi_0\rangle = |\sqrt{E}\rangle$, and $|\psi_1\rangle = |-\sqrt{E}\rangle$. The relevant parameters that determine channel performance are the fidelity

$$F(W) \equiv |\langle\psi_0|\psi_1\rangle|^2 = e^{-4E}, \tag{1}$$

and the symmetric Holevo information[4] $I(W) \equiv H(\rho)$, with $\rho \equiv 1/2(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|)$, where the von Neumann entropy $H(\sigma) \equiv -\text{Tr}\{\sigma\log_2\sigma\}$. The ultimate capacity achievable by the binary ensemble $|\psi_x\rangle$, $x \in \{0,1\}$, is given by the Holevo information of the average state $\rho_p \equiv p|\psi_0\rangle\langle\psi_0| + (1-p)|\psi_1\rangle\langle\psi_1|$ maximized over the prior $p \in [0,1]$, i.e., $C = \max_p H(\rho_p)$. The maximum for BPSK encoding is attained at $p = 1/2$. Therefore, the symmetric Holevo information is the Holevo capacity, $I(W) = H_2\left[\left(1+\sqrt{F(W)}\right)/2\right]$. Thus, for the BPSK alphabet, the Holevo capacity is given by:

$$C_\infty(E) = H_2\left[\left(1+e^{-2E}\right)/2\right], \tag{2}$$

where the subscript (∞) signifies that in order to achieve this capacity, the receiver must make collective measurements over long codeword blocks of an optimal binary code.

[1] In this paper, we will use the term "energy" to mean photon number. We are implicitly assuming a quasi-monochromatic light source with center frequency ω_0, for which mean photon number is indeed proportional to energy (with a proportionality factor of $\hbar\omega_0$).

[2] A general pure state of the temporal mode $s(t)$ is a unit-norm vector $|\psi\rangle = \sum_{n=0}^{\infty} c_n|n\rangle \in \mathcal{H}$, where $\{|n\rangle\}$ are quantum photon-number (Fock) states, which form a complete orthonormal basis of the Hilbert space $\mathcal{H}$. For a laser pulse, $c_n = \alpha^n e^{-|\alpha|^2/2}/\sqrt{n!}$ (photon number is Poisson-distributed with mean $|\alpha|^2$), and $|\psi\rangle$ in turn is the "coherent state" $|\alpha\rangle$.

[3] The subscript "1" in $C_1(E)$ signifies that it is the highest capacity achievable using a single-symbol detection, for the BPSK alphabet.

[4] The Holevo information reduces to the von Neumann entropy for a pure-state ensemble. More generally, if the channel outputs are mixed states ρ_0 and ρ_1, the fidelity is defined as $F(W) \equiv \left\|\sqrt{\rho_0}\sqrt{\rho_1}\right\|_1^2$, and the symmetric Holevo information as $I(W) \equiv H((\rho_0+\rho_1)/2) - H(\rho_0)/2 - H(\rho_1)/2$.

It is well-known that for $E \gg 1$, a coherent-state modulation along with standard (symbol-by-symbol) heterodyne detection asymptotically achieves the ultimate Holevo capacity $g(E)$ bits/symbol [1], and that the capacity gap between conventional single-symbol receivers and the Holevo limit is the highest at low photon numbers ($E \ll 1$) [2]. Hence, for the rest of this paper, we will focus on this $E \ll 1$ regime. The energy efficiency $C_1(E)/E$ (bits/photon) of the BPSK channel, when the best single-symbol detection is used on each channel output symbol, caps off at 2 nats/photon (2.89 bits/photon) as $E \to 0$. On the other hand, the Holevo limit to the energy efficiency of BPSK, $\lim_{E\to 0} C_\infty(E)/E = -\ln E + 1 + E \ln E + [\cdots]$ nats/photon [13] (where $[\cdots]$ indicates higher order terms), not only goes to infinity as $E \to 0$, but also approaches the ultimate (unrestricted-modulation) Holevo limit $g(E)/E$ asymptotically (see Fig. 1). The highest capacity (thus energy efficiency) with a BPSK modulation using a conventional receiver is achieved by ideal homodyne detection (see green plot in Fig. 1). Even though intensity modulation formats can attain an unbounded energy efficiency using a direct detection receiver, at low E (we will come back to this in Section II-1), at $E \ll 1$, a BPSK code—along with a JDR—is capable of practically closing the gap all the way to the ultimate limit to capacity (which is not possible by an intensity-only modulation).

So, how do we understand this huge gap between the best single-symbol Shannon capacity and the Holevo capacity of the BPSK alphabet (gap shown by the arrow in Fig. 1)? The two coherent states $\{|\sqrt{E}\rangle, |-\sqrt{E}\rangle\}$ are non-orthogonal (and thus not distinguishable), with inner product $e^{-2E} > 0$ as in (1). However, by virtue of the HSW theorem [6], the joint quantum states of well-chosen (i.i.d. random) 2^{NR} sequences of these two states (codeword waveforms) become nearly perfectly distinguishable as $N \to \infty$ as long as $R < C_\infty(E)$. Since these codeword states live in the N-symbol Hilbert space $\mathcal{H}^{\otimes N}$, a collective measurement is required to discriminate these states at a vanishingly low error rate. If the best single-symbol detection is used to detect each output BPSK symbol (thereby inducing a BSC and *we stress that this is the case with Arikan's polar encoding and classical successive cancellation decoder applied to the optical channel*), then an ML decoding can map the output *classical sequence* of these N binary-outcome measurements to the correct codeword with a vanishingly low probability of error, however only as long as $R < C_1(E)$ (i.e., it can sustain a lower capacity). Classical information theory works with the classical-input to classical-output "channel", which is determined by the combination of the physical transmission medium *and* the choice of the receiver measurement. Quantum information theory, in this case the HSW theorem, provides us with a tool to evaluate the best achievable capacity by automatically optimizing over all physically-realizable receiver measurements.

Unfortunately however, just like Shannon theory, the HSW theorem neither gives us a prescription to construct good low-complexity codes nor does it tell us how to realize the capacity-achieving receiver. In Section II, we provide the first explicit code (and a sequential-decoding collective measurement) that can achieve the BPSK Holevo capacity, the *classical-quantum polar code*.

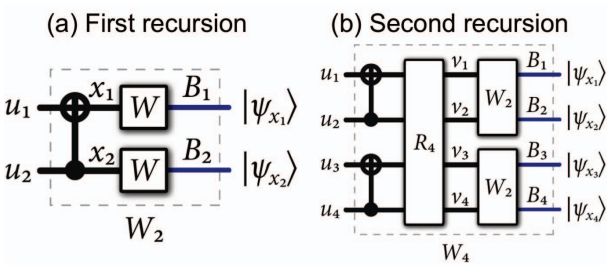

Fig. 2. (a) The channel W_2 synthesized from the first level of recursion. Thick lines denote classical systems while thin lines quantum systems. The gate shown is a CNOT, $(u_1, u_2) \to (u_1 \oplus u_2, u_2)$. (b) The second level of recursion in the channel combining phase. The operation R_4 simply permutes the bits so that all odd-index bits are first and all even-index bits are last.

II. Achieving the Holevo capacity of the binary pure-state quantum channel using a polar code

We now demonstrate how to construct a polar code for the binary pure-state channel (a special case being the BPSK optical channel), by appealing to our recent results on cq-polar codes for sending classical data over a quantum channel. These codes achieve the symmetric Holevo information rate for a general (potentially mixed-state) binary input alphabet [3].

Consider the binary pure-state classical-quantum channel $W : x \to |\psi_x\rangle$, $x \in \{0, 1\}$. Channels with fidelity $F(W) \leq \epsilon$ are nearly noiseless and those with $F(W) \geq 1 - \epsilon$ are near to being completely useless. Recall that the quantum fidelity is a generalization of the classical Bhattacharya distance Z [14], [3]. Let us consider $N = 2^n$ copies of W, such that the resulting channel is of the form: $x^N \equiv x_1 \cdots x_N \to |\psi_{x^N}\rangle \equiv |\psi_{x_1}\rangle \otimes \cdots \otimes |\psi_{x_N}\rangle$, where x^N is the length N input and $|\psi_{x^N}\rangle$ is the output state. We can extend Arikan's idea of channel combining [14] to this classical-quantum channel, by considering the channels induced by a transformation on an input bit (row) vector $u^N \to |\psi_{u^N G_N}\rangle$, where $G_N = B_N F^{\otimes n}$, with B_N being a permutation matrix that reverses the order of the bits and $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. This encoding is equivalent to a network of classical CNOT gates and permutations that can be implemented with complexity $O(N \log N)$. See Fig. 2 for the first and second instances of this encoding. Further instances are constructed recursively. We then define "split channels" from the above combined channels as:

$$W_N^{(i)} : u_i \to \rho_{(i),u_i}^{U_1^{i-1} B^N}, \tag{3}$$

where,

$$\rho_{(i),u_i}^{U_1^{i-1} B^N} \equiv \sum_{u_1^{i-1}} \frac{1}{2^{i-1}} |u_1^{i-1}\rangle\langle u_1^{i-1}|^{U_1^{i-1}} \otimes \overline{\rho}_{u_1^i}^{B^N}, \tag{4}$$

$$\overline{\rho}_{u_1^i}^{B^N} \equiv \sum_{u_{i+1}^N} \frac{1}{2^{N-i}} |\psi_{u^N G_N}\rangle\langle\psi_{u^N G_N}|^{B^N}. \tag{5}$$

The interpretation of this channel is that it is the one "seen" by the bit u_i if all the previous bits u_1^{i-1} are available and if all the future bits u_{i+1}^N as randomized. This motivates the development of a quantum successive cancellation decoder [3] that tries to distinguish $u_i = 0$ from $u_i = 1$ by adaptively exploiting the results of past measurements and Helstrom-Holevo measurements [15], [16] for each bit decision.

Arikan's polar coding rule divides the channels into "good" ones and "bad" ones [14]. Let $[N] \equiv \{1, \ldots, N\}$ and $0 < \beta < 1/2$. The polar coding rule for the classical-quantum channel divides the channels as follows:

$$\mathcal{A} \equiv \left\{ i \in [N] : \sqrt{F(W_N^{(i)})} < 2^{-N^\beta} \right\}, \tag{6}$$

so that the channels in $\mathcal{A}$ are the good ones and those in $\mathcal{A}^c$ are the bad ones. Observe that the quantum polar coding rule involves the quantum fidelity parameter $F(\cdot)$, rather than a classical one such as the Bhattacharya distance.

The following theorem is helpful in determining what fraction of the channels become good or bad [17]:

Theorem 1 (Convergence Rate): Let $\{X_n : n \geq 0\}$ be a random process with $0 \leq X_n \leq 1$ and satisfying

$$X_{n+1} \leq q X_n \quad \text{w.p.} \quad 1/2, \tag{7}$$
$$X_{n+1} = X_n^2 \quad \text{w.p.} \quad 1/2, \tag{8}$$

where q is some positive constant. Let $X_\infty = \lim_{n\to\infty} X_n$ exist almost surely with $\Pr\{X_\infty = 0\} = P_\infty$. Then for any $\beta < 1/2$, $\lim_{n\to\infty} \Pr\{X_n < 2^{-2^{n\beta}}\} = P_\infty$, and for any $\beta > 1/2$, $\lim_{n\to\infty} \Pr\{X_n > 2^{-2^{n\beta}}\} = 0$.

The channel combining and splitting mentioned above can be considered as a random birth process in which a channel W_{n+1} is constructed from two copies of a previous one W_n according to the rules in Section 4 of Ref. [3]. One can then consider the process $\{F_n : n \geq 0\} \equiv \{\sqrt{F(W_n)} : n \geq 0\}$ and prove that it is a bounded super-martingale by exploiting the relationships given in Proposition 10 of Ref. [3]. From the convergence properties of martingales, it follows that F_∞ converges almost surely to a value in $\{0, 1\}$, and the probability that it equals zero is equal to the symmetric Holevo information $I(W)$. Furthermore, since the process F_n satisfies the relations in (7-8), the following proposition on the convergence rate of polarization holds:

Theorem 2: Given a binary input classical-quantum channel W and any $\beta < 1/2$, $\lim_{n\to\infty} \Pr\{F_n < 2^{-2^{n\beta}}\} = I(W)$.

One of our important advances in Ref. [3] was to establish that a quantum successive cancellation decoder performs well for polar coding over classical-quantum channels with equiprobable inputs. Corresponding to the split channels $W_N^{(i)}$ in (3) are the following projectors that attempt to decide whether the input of the i^{th} split channel is zero or one:

$$\Pi_{(i),0}^{U_1^{i-1}B^N} \equiv \left\{ \rho_{(i),0}^{U_1^{i-1}B^N} - \rho_{(i),1}^{U_1^{i-1}B^N} \geq 0 \right\},$$
$$\Pi_{(i),1}^{U_1^{i-1}B^N} \equiv I - \Pi_{(i),0}^{U_1^{i-1}B^N},$$

where $\{B \geq 0\}$ denotes the projector onto the positive eigenspace of a Hermitian operator B. After some calculations, we can readily see that

$$\Pi_{(i),0}^{U_1^{i-1}B^N} = \sum_{u_1^{i-1}} |u_1^{i-1}\rangle\langle u_1^{i-1}|^{U_1^{i-1}} \otimes \Pi_{(i),u_1^{i-1}0}^{B^N}, \tag{9}$$

where $\Pi_{(i),1}^{U_1^{i-1}B^N} = I - \Pi_{(i),0}^{U_1^{i-1}B^N}$, $\Pi_{(i),u_1^{i-1}0}^{B^N} \equiv \{\overline{\rho}_{u_1^{i-1}0}^{B^N} - \overline{\rho}_{u_1^{i-1}1}^{B^N} \geq 0\}$, $\Pi_{(i),u_1^{i-1}1}^{B^N} \equiv I - \Pi_{(i),u_1^{i-1}0}^{B^N}$.

The above observations lead to a decoding rule for a successive cancellation decoder similar to Arikan's [14]:

$$\hat{u}_i = \begin{cases} u_i & \text{if } i \in \mathcal{A}^c \\ h(\hat{u}_1^{i-1}) & \text{if } i \in \mathcal{A} \end{cases},$$

where $h(\hat{u}_1^{i-1})$ is the outcome of the following i^{th} (collective) measurement on the codeword received at the channel output (after $i-1$ measurements have already been performed): $\{\Pi_{(i),\hat{u}_1^{i-1}0}^{B^N}, \Pi_{(i),\hat{u}_1^{i-1}1}^{B^N}\}$. We are assuming that the measurement device outputs "0" if the outcome $\Pi_{(i),\hat{u}_1^{i-1}0}^{B^N}$ occurs and it outputs "1" otherwise. (Note that we can set $\Pi_{(i),\hat{u}_1^{i-1}u_i}^{B^N} = I$ if the bit u_i is a frozen bit.) The above sequence of measurements for the whole bit stream u^N corresponds to a positive operator-valued measure (POVM) $\{\Lambda_{u^N}\}$ where

$$\Lambda_{u^N} \equiv \Pi_{(1),u_1}^{B^N} \cdots \Pi_{(i),u_1^{i-1}u_i}^{B^N} \cdots \cdots \Pi_{(N),u_1^{N-1}u_N}^{B^N} \cdots \Pi_{(i),u_1^{i-1}u_i}^{B^N} \cdots \Pi_{(1),u_1}^{B^N},$$

and $\sum_{u_\mathcal{A}} \Lambda_{u^N} = I^{B^N}$.

The probability of error $P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ for code length N, number K of information bits, set $\mathcal{A}$ of information bits, and choice $u_{\mathcal{A}^c}$ for the frozen bits is as follows:

$$P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c}) = 1 - \frac{1}{2^K} \sum_{u_\mathcal{A}} \text{Tr}\{\Lambda_{u^N} \rho_{u^N}\},$$

where we are assuming a particular choice of the bits $u_{\mathcal{A}^c}$ in the sequence of projectors $\Pi_{(N),u_1^{N-1}u_N}^{B^N} \cdots \Pi_{(i),u_1^{i-1}u_i}^{B^N} \cdots \Pi_{(1),u_1}^{B^N}$ and $\Pi_{(i),u_1^{i-1}u_i}^{B^N} = I$ if u_i is a frozen bit. We are also assuming that the sender transmits the information sequence $u_\mathcal{A}$ with uniform probability 2^{-K}. The probability of error averaged over all choices of the frozen bits is then,

$$P_e(N, K, \mathcal{A}) = \frac{1}{2^{N-K}} \sum_{u_{\mathcal{A}^c}} P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c})$$

The following proposition from Ref. [3] determines the average ensemble performance of polar codes with a quantum successive cancellation decoder:

Proposition 3: For any classical-quantum channel W with binary inputs and quantum outputs and any choice of $(N, K, \mathcal{A})$, the following bound holds

$$P_e(N, K, \mathcal{A}) \leq 2 \sqrt{\sum_{i \in \mathcal{A}} \frac{1}{2} \sqrt{F(W_N^{(i)})}}.$$

We proved the above bound on the performance of our SC decoder by exploiting Sen's "non-commutative union bound" [10] and Lemma 3.2 of Ref. [18] (which upper bounds the probability of error in a binary quantum hypothesis test by the fidelity between the test states). The bound holds under the assumption that the sender chooses the information bits $U_{\mathcal{A}}$ from a uniform distribution. Thus, by choosing the channels over which the sender transmits the information bits to be in $\mathcal{A}$ and those over which she transmits agreed-upon frozen bits to be in $\mathcal{A}^c$, we obtain the following bound on the probability of decoding error, as long as the code rate $R = K/N < I(W)$: $\Pr\{\widehat{U}_{\mathcal{A}} \neq U_{\mathcal{A}}\} = o(2^{-\frac{1}{2}N^{\beta}})$. This completes the specification of a cq polar code.

1) Polar codes for q-ary input channels: The binary *on-off keying* (OOK) alphabet $\left\{|0\rangle, |\sqrt{E_0}\rangle\right\}$ with priors $(1-p^*, p^*)$, $E = p^* E_0$, with optimal $p^*(E) \approx -E \ln E/3$, $E \ll 1$, along with a (symbol-by-symbol) direct detection (DD) receiver, attains a photon efficiency $C_{\mathrm{OOK-DD}}(E)/E = -\ln E - \ln\ln(1/E) + [\cdots]$ nats/photon [13] (magenta solid plot in Fig. 1). Furthermore, the Holevo capacity of the OOK alphabet is attained by $p^*(E) \approx \sqrt{E/2}$, and the photon efficiency is given by $C_{\mathrm{OOK-Holevo}}(E)/E = -\ln E + 1 + \sqrt{2}E^{1/2}\ln E + [\cdots]$ nats/photon (solid red plot in Fig. 1). At $E \ll 1$, a q-ary PPM constellation (which can be seen as a rate-$(\log_2 q)/q$ code over an underlying OOK alphabet) achieves a Shannon capacity (with DD) and a Holevo capacity, which are both extremely close to the respective unrestricted OOK capacities (dashed magenta and red plots in Fig. 1) respectively.

The q-ary PPM constellation achieves its capacity (both DD-Shannon and Holevo) for a uniform prior over its q inputs, forming a q-ary input classical-quantum channel. If q is a power of two, then a polar coding strategy to achieve the Holevo limit of PPM is straightforward, following the strategy to polar code for a uniform-input q-ary classical DMC (which can in turn achieve the PPM-DD capacity) [19]. Suppose that $m \equiv \log_2(q)$. Then one can decompose the input variable X as an m-fold Cartesian product of binary variables $(X_1, \ldots, X_m)$ and exploit a polar code for each of these variables. One first exploits a quantum successive cancellation (SC) decoder to decode the variable X_1 under the assumption that the other variables X_2, $\ldots$, X_m are chosen uniformly at random (and *thus are independent*) for this first step. This decoding achieves a low probability of error as long as the indices for the information bits are chosen according to the polar coding rule for this first induced channel. After decoding X_1, the quantum measurement could potentially disturb the state at the channel output, but this disturbance will be asymptotically small if the measurement successfully decodes (a result known as the Gentle Measurement Lemma [20]). Then, X_1 is available as side information for decoding the next variable X_2, and the procedure extends iteratively by decoding the current variable X_i with the previous i ones available as side information and randomizing over the future $m-i$ variables. The rate achieved with this scheme is equal to the symmetric Holevo capacity, by exploiting the chain rule and independence: $I(X_1 \cdots X_m; B) = \sum_{i=1}^{m} I(X_i; B X_1^{i-1})$.

III. Discussions and Conclusion

Our polar code and decoder construction in Ref. [3] offers the first near-explicit construction that almost closes the gap to the Holevo capacity limit for low-photon-number (high photon-efficiency) optical communications. Our construction improves upon earlier schemes by providing an explicit linear code with an efficient encoder (as opposed to a random code), while exponentially reducing the number of decoding steps (NR steps as opposed to the 2^{NR} in Refs. [9], [11]).

Several practical questions remain unanswered, the most important one perhaps being an explicit design of our polar-decoding receiver, i.e., an optical circuit involving beamsplitters, phase-shifters, squeezers, and potentially one third-order Hamiltonian such as a Kerr interaction. In order to make this scheme practical, finding efficient means to compute the rate matched cq polar codes for quantum channels would be necessary. Finally, it would be interesting to find an efficient classical-quantum polar coding scheme that can handle non-uniform input priors (viz., to achieve the Holevo limit of the OOK modulation alphabet).

References

[1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical capacity of the lossy bosonic channel: the exact solution," *Physical Review Letters*, vol. 92, p. 027902, 2004.

[2] S. Guha, "Structured optical receivers to attain superadditive capacity and the holevo limit," *Phys. Rev. Lett.*, vol. 106, p. 240502, 2011.

[3] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," September 2011, arXiv:1109.2591.

[4] R. M. Gagliardi and S. Karp, *Optical Communications*. John Wiley & Sons, Inc., 1976.

[5] A. Martinez, "Spectral efficiency of optical direct detection," *J. Opt. Soc. Am. B*, vol. 24, p. 735, 2007.

[6] A. S. Holevo, "The capacity of a quantum channel with general signal states," *IEEE Transactions on Information Theory*, vol. 44, p. 269, 1998.

[7] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, "Classical information capacity of a quantum channel," *Physical Review A*, vol. 54, p. 1869, 1996.

[8] H. P. Yuen and M. Ozawa, "Ultimate information carrying limit of quantum systems," *Phys. Rev. Lett.*, vol. 70, pp. 363–366, Jan 1993.

[9] S. Lloyd, V. Giovannetti, and L. Maccone, "Sequential projective measurements for channel decoding," *Phys. Rev. Lett.*, vol. 106, p. 250501, 2011.

[10] P. Sen, "Achieving the Han-Kobayashi inner bound for the quantum interference channel by sequential decoding," 2011, arXiv:1109.0802.

[11] M. M. Wilde, S. Guha, S.-H. Tan, and S. Lloyd, "Explicit capacity-achieving receivers for optical communication and quantum reading," 2012, arXiv:1202.0518, *Accepted for ISIT 2012*.

[12] S. J. Dolinar, "An optimum receiver for the binary coherent state quantum channel," M.I.T. Res. Lab. Elec. QPR, Tech. Rep., 1973.

[13] H. W. Chung, S. Guha, and L. Zheng, "On capacity of optical channels with coherent detection," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2011.

[14] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[15] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, pp. 231–252, 1969.

[16] A. S. Holevo, "An analog of the theory of statistical decisions in noncommutative theory of probability," *Trudy Moscov Mat. Obsc.*, vol. 26, pp. 133–149, 1972.

[17] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Int. Symp. Inf. Theory*, Seoul, Korea, June 2009, pp. 1493–1495.

[18] M. Hayashi, *Quantum Information: An Introduction*. Springer, 2006.

[19] E. Sasoglu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," *IEEE Info. Theory Wkshp.*, pp. 144–148, 2009.

[20] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. on Inf. Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.