Structured Optical Receivers to Attain Superadditive Capacity and the Holevo Limit

Saikat Guha

Disruptive Information Processing Technologies group, Raytheon BBN Technologies, Cambridge, Massachusetts 02138, USA

(Received 10 January 2011; published 14 June 2011)

Attaining the ultimate (Holevo) limit to the classical capacity of a quantum channel requires the receiver to make joint measurements over long code-word blocks. For a pure-state channel, we show that the Holevo limit can be attained by a receiver that uses a multisymbol unitary transformation on the quantum code word followed by separable projective measurements. We show a concatenated coding and joint-detection architecture to approach the Holevo limit. We then construct some of the first concrete examples of codes and structured joint-detection receivers for the lossy bosonic channel, which can achieve fundamentally higher (superadditive) capacity than conventional receivers that detect each modulation symbol individually. We thereby pave the way for research into codes and structured receivers for reliable communication data rates approaching the Holevo limit.

DOI: 10.1103/PhysRevLett.106.240502 PACS numbers: 03.67.Hk, 42.50.Ex, 42.79.Sz

When the modulation alphabet of a communication channel is comprised of quantum states, the Holevo limit is an upper bound to the Shannon capacity of the physical channel paired with any receiver measurement. Even though the Holevo limit is an achievable capacity, the receiver in general must make joint (*collective*) measurements over long code-word blocks—measurements that cannot in general be realized by detecting single modulation symbols followed by classical postprocessing. This phenomenon of a joint-detection receiver (JDR) being able to yield higher capacity than any single-symbol receiver measurement is often termed as *superadditivity* of capacity. The more recent usage of the term superadditivity of capacity refers to a quantum channel being able to achieve a higher classical communications rate by using transmitted states that are entangled over multiple channel uses [1,2]. For the point-to-point lossy bosonic channel, we showed that entangled inputs at the transmitter cannot get a higher capacity [3]. However, one *can* get a higher capacity by using joint-detection measurements at the receiver (as opposed to a symbol-by-symbol optical receiver). In this Letter, we use the term superadditivity in this latter context. This usage of the term was first adopted by Sasaki *et al.* [4].

For the lossy bosonic channel (such as a free-space line-of-sight optical link between a pair of transmit and receive apertures), a coherent-state modulation suffices to attain the Holevo capacity; i.e., nonclassical transmitted states do not yield any additional capacity [3]. Hausladen *et al.*'s square-root measurement [5], which in general is a positive operator-valued measure (POVM), applied to a random code gives us the mathematical construct of a receiver that can achieve the Holevo limit. Lloyd, Giovannetti, and Macconne [6] recently showed a receiver that can attain the Holevo capacity of any quantum channel by making a sequence of "yes-no" projective measurements on a random code book. Sasaki *et al.* showed several examples of superadditive capacity by using pure-state alphabets and the square-root measurement [4]. However, the key practical questions that remain unanswered are how to design modulation formats, channel codes, and, most importantly, structured optical realizations of Holevo-capacity-approaching receivers.

In this Letter, we start by showing a simple result that the Holevo limit of a pure-state channel is attained by a projective measurement, which can be implemented by a unitary operation on the quantum code word followed by separable projective measurements on the single-modulation-symbol subspaces. Thereafter we translate this result into a concatenated coded receiver architecture for the lossy bosonic channel. Finally, we show concrete examples of codes and receivers pursuant to this architecture, which yield superadditive capacity for binary-phase-shift keying (BPSK) signaling at low photon numbers. These, we believe, are the first receiver realizations that can exhibit superadditivity and can be tested by using simple laboratory optics.

Attaining the Holevo limit of a pure-state channel.—We encode classical information by using a Q-ary modulation alphabet of nonorthogonal pure-state *symbols* in $\mathcal{A} \equiv \{|\psi_1\rangle, \ldots, |\psi_Q\rangle\}$. Each *channel use* constitutes sending one symbol. We assume that the channel preserves the purity of $\mathcal{A}$ and, thus, take the states $\{|\psi_q\rangle\}$ to be those at the receiver. The only source of noise is the physical detection of the states. Assume that the receiver detects each symbol one at a time. Channel capacity is given by the maximum of the single-symbol mutual information

$$C_1 = \max_{\{p_i\}} \max_{\{\hat{\Pi}_j^{(1)}\}} I_1(\{p_i\}, \{\hat{\Pi}_j^{(1)}\}) \text{ bits/symbol}, \tag{1}$$

where the maximum is taken over priors $\{p_i\}$ over the alphabet and a set of POVM operators $\{\hat{\Pi}_j^{(1)}\}$, $1 \leq j \leq J$, on the single-symbol state space. The measurement of each symbol produces one of J possible outcomes, with conditional probabilities $P(j|i) = \langle\psi_i|\hat{\Pi}_j^{(1)}|\psi_i\rangle$, which define a discrete memoryless channel. To achieve reliable communication on this channel at a rate close to C_1, forward error correction will be required. In other words, for any rate $R < C_1$, there exists a sequence of code books $\mathcal{C}_n$ with $K = 2^{nR}$ code words $|\mathbf{c}_k\rangle$, $1 \le k \le K$, each code word being an n-symbol tensor product of states in $\mathcal{A}$, and a decoding rule, such that the average probability of decoding error (guessing the wrong code word) $\bar{P}_e^{(n)} = 1 - \frac{1}{K} \times \sum_{k=1}^{K} \Pr(\hat{k} = k) \to 0$, as $n \to \infty$. In this "Shannon" setting, optimal decoding is a maximum likelihood (ML) decision, which can in principle be precomputed as a long table lookup (see Fig. 1), although a low-complexity channel decoder is desirable in any practical setting. Let us define C_n as the maximum capacity achievable (in bits per symbol) with measurements that jointly detect up to n symbols. The fact that joint detection allows for $(n+m)C_{n+m} > nC_n + mC_m$ (or $C_n > C_1$) is referred to as superadditivity of capacity. The Holevo-Schumacher-Westmorland theorem says

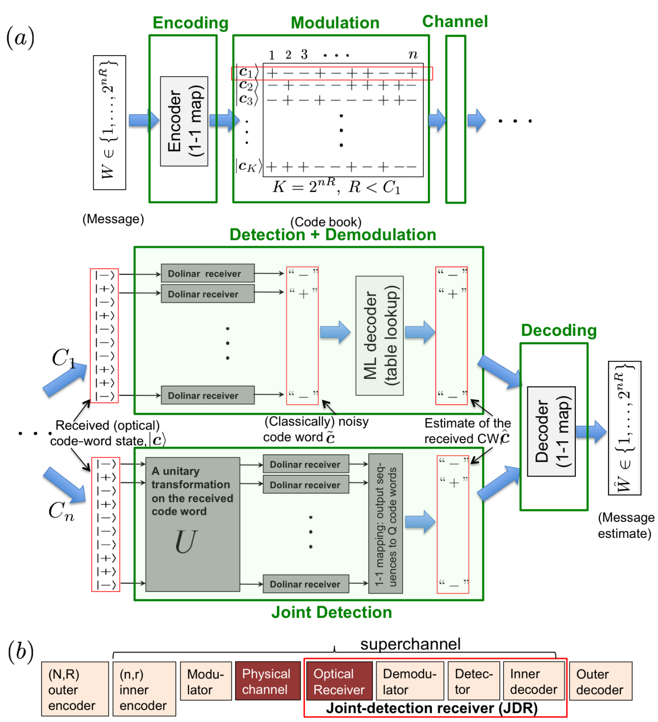

FIG. 1 (color online). (a) Classical communication system, shown here for a BPSK alphabet. If the receiver uses symbol-by-symbol detection, maximum capacity = C_1 bits/symbol. If the detection + demodulation block is replaced by a general n-symbol joint quantum measurement, maximum capacity = C_n bits/symbol. Superadditivity: $C_\infty > C_n > C_1$, where C_∞ is the Holevo limit. The joint-detection structure shown achieves the Holevo limit for a coherent-state BPSK modulation. (b) Our proposed modification of the classical concatenated coding architecture [9], in which the *channel* is broken up into the physical channel and a receiver measurement, with the joint-detection receiver acting on the inner code.

$$C_\infty \equiv \lim_{n\to\infty} C_n = \max_{\{p_i\}} S\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right), \tag{2}$$

the Holevo bound, is the ultimate capacity limit, where $S(\hat{\rho}) = -\mathrm{Tr}\hat{\rho}\log_2\hat{\rho}$ is the von Neumann entropy, and that C_∞ is achievable with joint detection over long code-word blocks. Calculating C_∞, however, does not require the knowledge of the optimal receiver measurement. In other words, if we replaced the detection and demodulation stages in Fig. 1(a) by one giant quantum measurement, then for any rate $R < C_\infty$, there exists a sequence of code books $\mathcal{C}_n$ with $K = 2^{nR}$ code words $|\mathbf{c}_k\rangle$, $1 \le k \le K$, and an n-input n-output POVM over the n-symbol state space $\{\hat{\Pi}_k^{(n)}\}$, $1 \le k \le K$, such that the average probability of decoding error $\bar{P}_e^{(n)} = 1 - \frac{1}{K}\sum_{k=1}^{K}\langle\mathbf{c}_k|\hat{\Pi}_k^{(n)}|\mathbf{c}_k\rangle \to 0$, as $n \to \infty$.

Theorem 1.—For a pure-state channel, a projective measurement can attain C_∞ and can be implemented as a unitary transformation on the code word followed by a parallel set of separable single-symbol measurements.

Proof.—The minimum probability of error (MPE) measurement for discriminating a set of pure-state code words is a projective measurement [7], which by definition obtains a lower probability of decoding error than the square-root measurement. Since the latter is known to be capacity-achieving for a large random code [5], the MPE measurement must also be so. Finally, it is straightforward to show that any projective measurement on the n-symbol state space can be implemented by a unitary transformation on the n-symbol code word (a tensor-product pure state) followed by a sequence of separable projective measurements on each symbol. ■

The Dolinar receiver [8] implements a binary projective MPE measurement to optimally distinguish two nonorthogonal coherent states. Therefore a capacity-achieving receiver for a binary coherent-state channel could be implemented as a unitary rotation of an n-symbol code word followed by a sequence of Dolinar receivers [Fig. 1(a)], which is in general a joint measurement. Despite the result of Theorem 1, finding optimal codes and low-complexity JDRs is difficult. It is common wisdom in classical coding theory that concatenated codes can approach Shannon capacity while requiring extremely low-complexity decoders, at the expense of a lower error exponent [i.e., longer code-word lengths (n) needed to attain a given $\bar{P}_e^{(n)}$, as compared to a single optimal code and the ML decoder] [9]. We propose a similar concatenated coding architecture—shown in Fig. 1(b)—to approach the quantum channel's Holevo capacity, where the JDR acts on the inner code to attain a superadditive Shannon capacity $C_n > C_1$, and the outer code (e.g., a Reed Solomon code) drives down the error rates to attain reliable communications at the capacity C_n of the inner "superchannel" [see Fig. 1(b)]. The remainder of this Letter will present two practical constructions of such superchannels that yield superadditive capacity.

Superadditive optical receivers.—Consider a single-mode lossy bosonic channel, where data are modulated by using a succession of pulses (orthogonal temporal modes) with mean received photon number $\bar{n}$ per mode, where each pulse carries one modulation symbol. The Holevo capacity $C_{\text{ult}}(\bar{n}) = g(\bar{n}) = (1+\bar{n})\log_2(1+\bar{n}) - \bar{n}\log_2\bar{n}$ bits/symbol, which is attained by using a coherent-state modulation [3]. Since pure loss preserves coherent states (with linear amplitude attenuation), it suffices to define capacity as a function of the mean photon number per *received* mode $\bar{n}$, and the pure-state channel discussion above applies. At high $\bar{n}$, symbol-by-symbol heterodyne detection asymptotically achieves the Holevo limit. The low photon number regime is more interesting, where the joint-detection gain is the most pronounced.

In Fig. 2, we show the photon information efficiency (PIE), the number of bits that can be reliably decoded per received photon, as a function of $\bar{n}$ [10]. There is no fundamental upper bound to the PIE; however, higher PIE necessitates lower $\bar{n}$. Furthermore, binary modulation and coding is sufficient to meet the Holevo limit at low $\bar{n}$. Specifically, the BPSK alphabet $\mathcal{A}_1 \equiv \{|\alpha\rangle, |-\alpha\rangle\}$, $|\alpha|^2 = \bar{n}$, is the Holevo-optimal binary modulation at $\bar{n} \ll 1$. The Dolinar receiver realizes the binary MPE measurement on any pair of coherent states by using single-photon detection and coherent optical feedback [8]. If the Dolinar receiver is used to detect each symbol, the BPSK channel is reduced to a classical binary symmetric channel with capacity $C_1 = 1 - H(q)$ bits/symbol, where $H(\cdot)$ is the binary Shannon entropy and $q = [1 - \sqrt{1 - e^{-4\bar{n}}}]/2$ is the minimum mean probability of error to discriminate $\{|\alpha\rangle, |-\alpha\rangle\}$. This is the maximum achievable capacity when the receiver detects each symbol individually, which includes all conventional (direct-detection and coherent-detection) receivers. The PIE $C_1(\bar{n})/\bar{n}$ caps out at $2/\ln 2 \approx 2.89$ bits/photon at $\bar{n} \ll 1$. Closed-form expressions and scaling behavior of C_n, the maximum capacity achievable with measurements that jointly detect up to n symbols, for $n \geq 2$ are not known. However, the Holevo limit of BPSK, $C_\infty(\bar{n}) = H([1 + e^{-2\bar{n}}]/2)$, can be calculated easily by using Eq. (2). Good codes and JDRs would be needed to bridge the huge gap between the PIEs $C_1(\bar{n})/\bar{n}$ and $C_\infty(\bar{n})/\bar{n}$, shown in Fig. 2. It is interesting to reflect on the point shown by the orange circle (at 10 bits/photon) in Fig. 2, which says that, for a 1.55 μm far-field free-space optical link operating at 1 GHz modulation bandwidth, the laws of physics permit reliable communication at 0.266 Gbps with only 3.4 pW of average (and peak) received optical power.

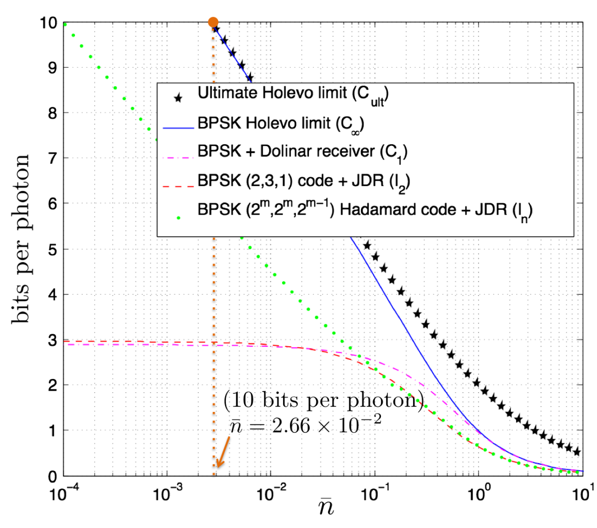

FIG. 2 (color online). Photon information efficiency (bits per received photon) as a function of mean photon number per mode, $\bar{n}$.

A two-symbol superadditive JDR.—Some examples of superadditive codes and joint measurements have been reported [4,11] but not with structured receiver designs. An ensemble [a (2, 3, 1) inner code [12]] containing three of the four 2-symbol BPSK states, $\mathcal{A}_2 \equiv \{|\alpha\rangle|\alpha\rangle, |\alpha\rangle|-\alpha\rangle, |-\alpha\rangle|\alpha\rangle\}$, with priors $(1-2p, p, p)$, $0 \leq p \leq 0.5$, can attain, with the best 3-element projective measurement in span($\mathcal{A}_2$), up to $\approx 2.8\%$ higher capacity that C_1 [11]. Since this is a Shannon capacity result, a classical outer code with code words comprising of sequences of states from $\mathcal{A}_2$ will be needed to achieve this capacity $I_2 > C_1$. By using the MPE measurement on $\mathcal{A}_2$ (which can be analytically calculated [7], unlike the numerically optimized projections in [11]), $I_2/C_1 \approx 1.0266$ can be obtained. We have found the first structured receiver that attains superadditivity. It involves a unitary operation on the (2, 3, 1) code (a beam splitter) followed by separable single-symbol measurements [in this case, a single-photon detector (SPD), and a Dolinar receiver] (see Fig. 3) and can attain $I_2/C_1 \approx 1.0249$ (see Fig. 2). It is likely that none of these projective measurements on $\mathcal{A}_2$ attain C_2, since the single-shot measurement that maximizes the accessible information in $\mathcal{A}_2$ could in general be a 6-element POVM [13].

An n-symbol superadditive JDR.—A $(2^m - 1, 2^m, 2^{m-1})$ BPSK Hadamard code with $\bar{n}$-mean-photons BPSK symbols is unitarily equivalent to the $(2^m, 2^m, 2^{m-1})$ pulse-position-modulation (PPM) code with $2^m\bar{n}$-mean-photon-number pulses. The former is slightly more *space-efficient*, since it achieves the same equidistant distance profile, but with one less symbol. Consider a BPSK Hadamard code detected by a 2^m-mode unitary transformation (with one ancilla mode, prepared locally at the

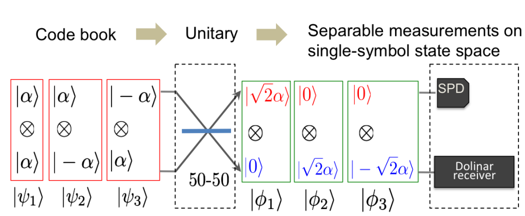

FIG. 3 (color online). A two-symbol JDR that attains $\approx 2.5\%$ higher capacity for BPSK than the best single-symbol (Dolinar) receiver.

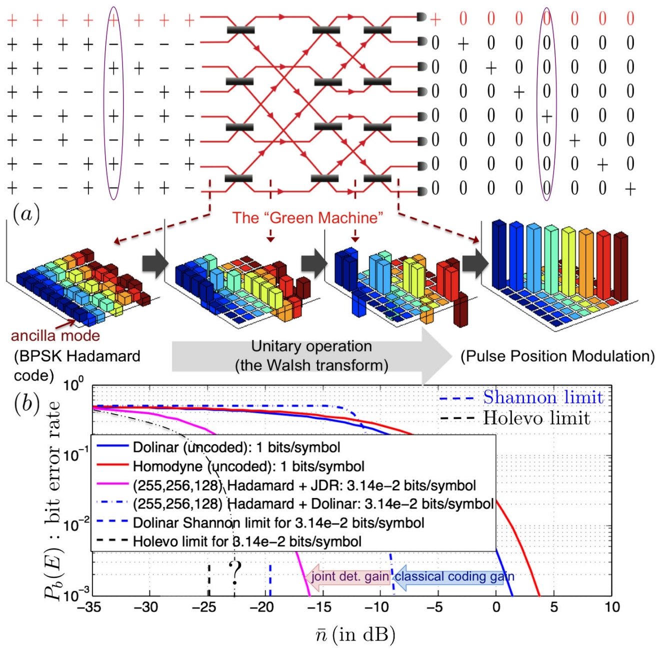

FIG. 4 (color online). (a) The BPSK (7, 8, 4) Hadamard code is unitarily equivalent to the (8, 8, 4) PPM code via a Green machine built by using 12 50-50 beam splitters. (b) Bit error rate plotted as a function of $\bar{n}$. The plot marked "?" is not the bit error rate for any known code-receiver pair; we just know that codes and physical joint-detection receivers that approach the Holevo limit must exist.

receiver, in the $|\alpha\rangle$ state) built by using $(n\log_2 n)/2$ 50-50 beam splitters arranged in the "Green machine" format, followed by a separable $n = 2^m$-element SPD array, as shown (for $n = 8$) in Fig. 4. The beam splitters unravel the BPSK code book into a PPM code book, collecting the photons into spatially separated bins. The ancilla mode necessitates a local oscillator phase locked to the received pulses, which is hard to implement. But we can append the ancilla mode to the transmitted code word, so that the received ancilla can serve as a pilot tone for our interferometric receiver. The Shannon capacity of this code-JDR superchannel—allowing for outer coding over the erasure outcome (i.e., no clicks registered by any detector)—is $I_n(\bar{n}) = (\log_2 K/K)[1 - \exp(-2d\bar{n})]$ bits/symbol, where $d = 2^{m-1}$. In Fig. 2, we plot the envelope $\max_n I_n(\bar{n})/\bar{n}$ (the green dotted plot) as a function of $\bar{n}$. This JDR not only attains a *much* higher superadditive gain than the $n = 2$ case we described above, it does not need phase tracking and coherent optical feedback like the Dolinar receiver. In Fig. 4(b), we plot the bit error rates $P_b(E)$ as a function of $\bar{n}$ for uncoded BPSK, and for the (255, 256, 128) BPSK Hadamard code, when detected by using both a symbol-by-symbol Dolinar receiver and our structured JDR, respectively. The *coding gain* now has two components, a (classical) coding gain and an additional *joint-detection gain*. In Ref. [14], we show a more involved JDR construction for the first-order Reed Muller codes, which attains higher superadditive capacity.

A great deal is known about binary codes that achieve low bit error rates on the binary symmetric channel at $\bar{n}$ very close to the Shannon limit [9]. It would be useful to design codes with symmetries that allow them to approach Holevo capacity, with the unitary U of the inner code's JDR in Fig. 1(a) realizable via a simple network of beam splitters, phase shifters, two-mode squeezers, and Kerr nonlinearities (which form a universal set for realizing an arbitrary multimode bosonic unitary [15]) along with a low-complexity outer code. The fields of information and coding theory have had a unique history. Even though many of its ultimate limits were determined in Shannon's founding paper [16], it took generations of magnificent coding theory research to ultimately find practical capacity-approaching codes. Even though realizing high-photon-efficiency communication on an optical channel close to the Holevo limit might take a while, it certainly does seem to be on the visible horizon.

This work was supported by the DARPA Information in a Photon program, Contract No. HR0011-10-C-0159. Discussions with Professors J. H. Shapiro, S. Lloyd, and L. Zheng, MIT, Dr. Z. Dutton, BBN, Drs. K. Bradler and M. Wilde, McGill University, and Dr. M. Neifeld, DARPA, are gratefully acknowledged.

[1] M. Hastings, Nature Phys., **5**, 255 (2009).
[2] L. Czekaj and P. Horodecki, Phys. Rev. Lett. **102**, 110505 (2009).
[3] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).
[4] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, Phys. Rev. A **58**, 146 (1998).
[5] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).
[6] S. Lloyd, V. Giovannetti, and L. Macconne, arXiv:1012.0106v1.
[7] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[8] S. J. Dolinar, Ph.D. thesis, MIT, 1976, http://dspace.mit.edu/handle/1721.1/27472.
[9] G. D. Forney, *Concatenated Codes* (MIT, Cambridge, MA, 1966).
[10] PIE is a more useful metric to communication engineers than channel capacity $C(\bar{n})$. It translates readily into a trade-off between *photon efficiency*, $C(\bar{n})/\bar{n}$ bits/photon, and *spectral efficiency*, $C(\bar{n})$ bits/ sec/Hz.
[11] J. R. Buck, S. J. van Enk, and C. A. Fuchs, Phys. Rev. A **61**, 032309 (2000).
[12] An *(n, K, d)* code has K length-*n* code words, such that the minimum Hamming distance between any pair of code words is d. The *code rate* is $R = \log_2 K/n$ bits/symbol.
[13] P. Shor, arXiv:quant-ph/0206058.
[14] S. Guha, Z. Dutton, and J. H. Shapiro, arXiv:1102.1963v1.
[15] S. Sefi and P. Loock, arXiv:1010.0326v1.
[16] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).