Structured Optical Receivers to Attain Superadditive Capacity and the Holevo Limit

Saikat Guha

Phys. Rev. Lett. **106**, 240502 — Published 14 June 2011

DOI: 10.1103/PhysRevLett.106.240502

Structured optical receivers to attain superadditive capacity and the Holevo limit

Saikat Guha
Disruptive Information Processing Technologies group,
Raytheon BBN Technologies, Cambridge, MA 02138, USA

When classical information is sent over a quantum channel, attaining the ultimate limit to channel capacity requires the receiver to make joint measurements over long codeword blocks. For a pure-state channel, we show that the ultimate (Holevo) limit to capacity can be attained by a receiver that uses a multi-symbol unitary transformation on the received quantum codeword followed by separable projective measurements on the single-modulation-symbol state spaces. We study the ultimate limits of photon-information-efficient communications on a lossy bosonic channel, and show a general concatenated coding and joint detection architecture to approach the Holevo limit to capacity. Based on our general results for the pure-state quantum channel, we show some of the first concrete examples of codes and structured joint-detection optical receivers that can achieve fundamentally higher (superadditive) channel capacity than conventional receivers that detect each modulation symbol individually. We thereby pave the way for future research into codes and structured optical receivers that can attain reliable communications at data rates approaching the Holevo limit.

When the modulation alphabet of a communication channel comprise 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*, or *entangling*) measurements over long codeword blocks—measurements that can't in general be realized by detecting single modulation symbols followed by classical post processing. 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 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., non-classical 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 et. al. [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 codebook. Sasaki et. al. [4], in a series of papers, showed several examples of superadditive capacity using pure-state alphabets and the square-root measurement. 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 codeword 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 superaddivity, and can be tested using simple laboratory optics.

Attaining Holevo limit of a pure-state channel. We encode classical information using a Q-ary modulation alphabet of non-orthogonal 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 $\mathcal{A}$, thus take the states $\{|\psi_q\rangle\}$ to be those at the receiver. 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,

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

where the maximum is taken over priors $\{p_i\}$ over the alphabet and a set of POVM operators $\left\{\hat{\Pi}_j^{(1)}\right\}$, $1 \le j \le J$ 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 de-

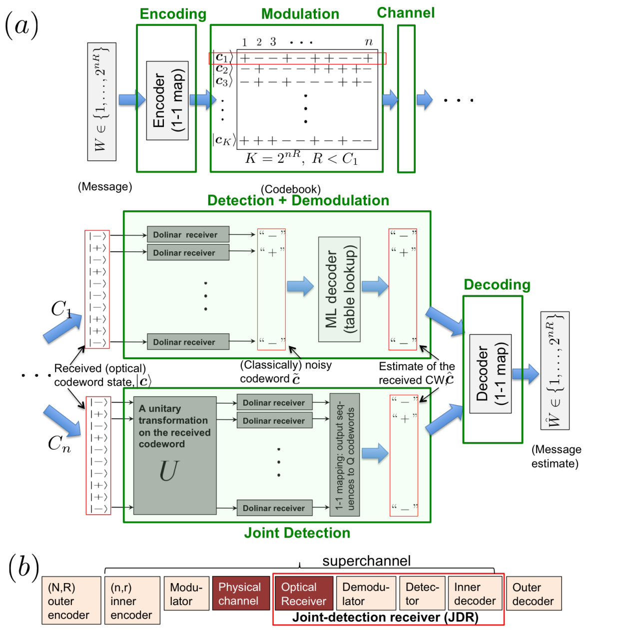

FIG. 1: (a) Classical communication system, shown here for a BPSK alphabet. If the receiver uses symbol-by-symbol detection, maximum capacity $= C_1$ bits/symbol. If the Detection+Demodulation block is replaced by a general n-symbol joint quantum measurement, maximum capacity $= C_n$ bits/symbol. Superadditivity: $C_\infty > C_n > C_1$, 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 [7], 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.

fine 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 codebooks $\mathcal{C}_n$ with $K = 2^{nR}$ codewords $|\boldsymbol{c}_k\rangle$, $1 \le k \le K$, each codeword 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 codeword), $\bar{P}_e^{(n)} = 1 - \frac{1}{K}\sum_{k=1}^{K} \Pr(\hat{k} = k) \to 0$, 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 (HSW) theorem says,

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

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 codeword blocks. Calculating C_∞ however, doesn't 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 codebooks $\mathcal{C}_n$ with $K = 2^{nR}$ codewords $|\boldsymbol{c}_k\rangle$, $1 \le k \le K$, and an n-input n-output POVM over the n-symbol state-space $\left\{\hat{\Pi}_k^{(n)}\right\}$, $1 \le k \le K$, such that the average probability of decoding error, $\bar{P}_e^{(n)} = 1 - \frac{1}{K}\sum_{k=1}^{K}\langle\boldsymbol{c}_k|\hat{\Pi}_k^{(n)}|\boldsymbol{c}_k\rangle \to 0$, 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 codeword followed by a parallel set of separable single-symbol measurements.*

Proof. The proof follows from the simple observation that the minimum probability of error (MPE) measurement for discriminating a set of pure state codewords is a projective measurement [8], which by definition, must obtain a lower probability of decoding error than the square root measurement. Given 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 first applying a unitary transformation on the n-symbol quantum codeword (a tensor-product pure state) followed by a sequence of separable projective measurements on each symbol. □

The Dolinar receiver [9] implements a binary projective MPE measurement to optimally distinguish two non-orthogonal coherent states. Therefore a capacity achieving receiver for a binary coherent state channel could be implemented as a unitary rotation of an n-symbol codeword 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 that can be built using structured optics 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 codeword lengths (n) needed to attain a given $\bar{P}_e^{(n)}$, as compared to a single optimal code and the ML decoder) [7]. 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

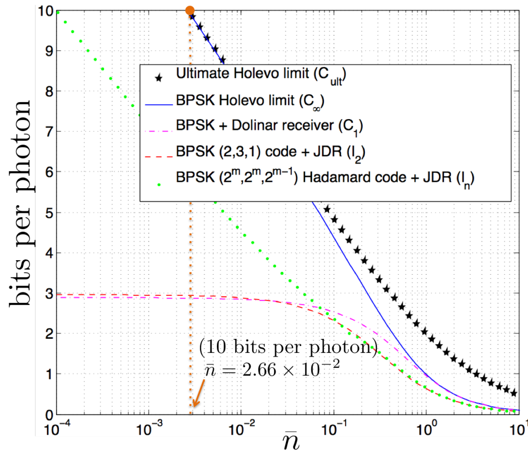

FIG. 2: Photon information efficiency (bits per received photon) as a function of mean photon number per mode, $\bar{n}$.

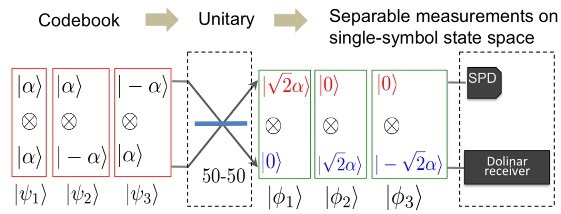

FIG. 3: A two-symbol JDR that attains $\approx 2.5\%$ higher capacity for BPSK than the best single-symbol (Dolinar) receiver.

present two practical constructions of such superchannels that demonstrate superadditive capacity ($C_n > C_1$).

Superadditive optical receivers. Consider a single-mode lossy bosonic channel (such as a far-field single-spatial-mode free-space-optical channel), where data is modulated 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, $C_{\rm ult}(\bar{n}) = g(\bar{n}) = (1+\bar{n})\log_2(1+\bar{n}) - \bar{n}\log_2\bar{n}$ bits/symbol, which is attained 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 $\bar{n}$ [15]. 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 $\bar{n} \ll 1$. Dolinar proposed a structured receiver that realizes the binary MPE projective measurement on an a pair of coherent states using single photon detection and coherent optical feedback [9]. 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 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 1.55μm far-field free-space optical link operating at 1 GHz modulation bandwidth, the laws of physics permit reliable communications at 0.266 Gbps with only 3.4 pW of average (and peak) received optical power!

A two-symbol superadditive JDR— Some examples of superadditive codes and joint measurements have been reported [4, 10], but not with structured receiver designs. An ensemble (a $(2,3,1)$ inner code [16]) 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 [10]. Since this is a Shannon capacity result, a classical outer code with codewords comprising of sequences of states from $\mathcal{A}_2$ will be needed to achieve this capacity $I_2 > C_1$. Using the MPE measurement on $\mathcal{A}_2$ (which can be analytically calculated [8], unlike the numerically optimized projections in [10]), $I_2/C_1 \approx 1.0266$ 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 beamsplitter) followed by two 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). Its 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 [11].

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—over an underlying on-off-keying binary signaling alphabet—with $2^m\bar{n}$-

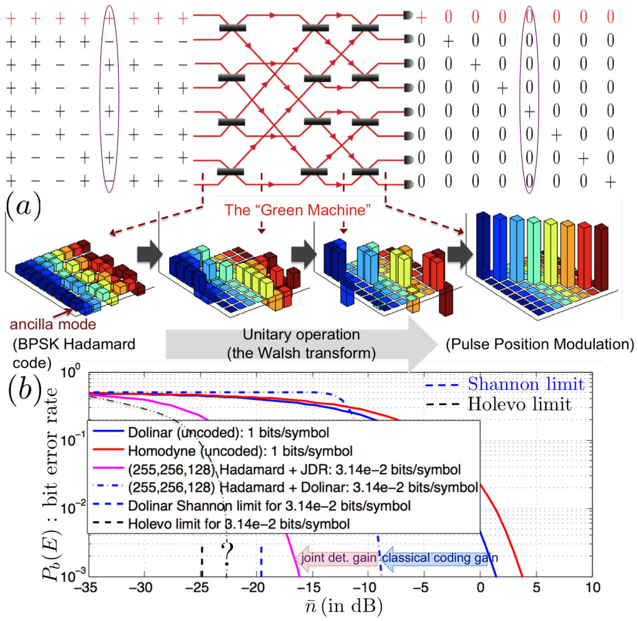

FIG. 4: (a) The BPSK $(7, 8, 4)$ Hadamard code is unitarily equivalent to the $(8, 8, 4)$ pulse-position-modulation (PPM) code via a “Green Machine” built using twelve 50-50 beam-splitters. (b) Bit error rate plotted as a function of $\bar{n}$. The plot marked “?” is not the bit error rate for any known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

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 receiver, in the $|\alpha\rangle$ state) built 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 codebook into a PPM codebook, separating the photons into spatially-separate bins. This receiver may be a more natural choice for spatial modulation across n orthogonal spatial modes of a near-field free-space channel. The ancilla mode at the receiver necessitates a local oscillator phase locked to the received pulses, which is hard to implement. Since the number of ancilla modes doesn't scale with the size of the code, we can append the ancilla mode to the transmitted codeword, 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. 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[17]. 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, both when detected using 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 [12], 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 [7]. It would be interesting to see how close to the Holevo limit can these same codes perform, when paired with their respective quantum MPE measurements. It will 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 non-linearities (which form a universal set for realizing an arbitrary multimode bosonic unitary [13]) 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 [14], it took generations of magnificent coding theory research to ultimately find practical capacity-approaching codes. Even though realizing high-photon-efficiency communications on an optical channel close to the Holevo limit might take a while, it certainly does seem to be in the visible horizon.

This work was supported by the DARPA Information in a Photon program, contract#HR0011-10-C-0159. Discussions with Profs. Jeffrey H. Shapiro, Seth Lloyd, and Lizhong Zheng, MIT, Dr. Zachary Dutton, BBN, Drs. Kamil Bradler and Mark Wilde, McGill Univ., and Dr. Mark Neifeld, DARPA are gratefully acknowledged.

[1] M. Hastings, Nature Physics, Vol. 5, 4, 255-257 (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, H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).
[4] M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Phys. Rev. A **58**, 146 (1998).
[5] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).
[6] S. Lloyd, V. Giovannetti, L. Macconne, arXiv:1012.0106v1 [quant-ph], (2010).
[7] G. D. Forney, *Concatenated Codes*, MIT Press, Cambridge, MA, (1966).
[8] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic, New York, (1976).
[9] S. J. Dolinar, Ph.D. thesis, MIT (1976).
[10] J. R. Buck, S. J. van Enk, C. A. Fuchs, Phys. Rev. A **61**, 032309, (2000).
[11] P. Shor, arXiv:0206058v3 [quant-ph], (2003).
[12] S. Guha, Z. Dutton, J. H. Shapiro, Proc. ISIT (2011).

[13] S. Sefi, P. Loock, arXiv:1010.0326v1 [quant-ph], (2010).

[14] C. E. Shannon, *Bell System Technical Journal* **27**, (1948).

[15] PIE is a more useful metric to communication engineers than channel capacity $C(\bar{n})$. It translates readily into a tradeoff between *photon efficiency*, $C(\bar{n})/\bar{n}$ bits/photon, and *spectral efficiency*, $C(\bar{n})$ bits/sec/Hz.

[16] An (n, K, d) code has K length-n codewords, such that the minimum Hamming distance between any pair of codewords is d. The *code rate* is $R = \log_2 K/n$.

[17] Note that n-ary PPM signaling also achieves $I_n(\bar{n})$ with an SPD, albeit with a much higher ($\times 2^m$) peak power as compared to BPSK. However, the receiver construct shown in Fig. 1(a) is capable of bridging the rest of the gap to the Holevo limit (i.e., the blue solid plot in Fig. 2) using an optimal BPSK code (minimum possible peak power) and a JDR.