LDPC-Coded $M$-ary PSK Optical Coherent State Quantum Communication

Ivan B. Djordjevic, Member, IEEE

Abstract—This paper addresses two important problems of interest for deep-space optical communications, quantum inter-chip/intra-chip optical communications and quantum-key distribution: 1) the problem of coded $M$-ary phase-shift keying optical coherent-state quantum communication in the absence of background radiation, and 2) the problem of coded binary coherent state communication in the presence of background radiation. In both cases large girth low-density parity-check (LDPC) codes are used as channel codes. With girth-10 LDPC-code of rate 0.8 and BPSK, the bit-error ratio of $10^{-8}$ can be achieved for average number of signal photons of 0.73, resulting in net-effective coding gain of 7.63 dB.

Index Terms—Coherent-state quantum communications, low-density parity-check (LDPC) codes, $M$-ary phase-shift keying (PSK), on-off keying (OOK), optical communications, quantum communications.

I. INTRODUCTION

The quantum information processing is an interesting research area with variety of applications, ranging from cryptography to complexity theory [1]. However, it relies on fragile superposition states required to manipulate the quantum information, and are very sensitive to the decoherence effect. The recent experimental verification by Cook et al. [2] of long-standing theoretical prediction due to Helstrom [3], has confirmed that the laser lightwave communication is a convenient quantum system for transmission of information, which in combination with coherent state discrimination by real-time quantum feedback [2], [4] can be used instead of delicate entanglement measurement [5] or quantum superposition [1].

The purpose of this paper is twofold. First we study the improvements that can be obtained by employing the high-rate structured low-density parity-check (LDPC) codes [6]–[8], if Dolinar-like quantum receivers [9] are employed. We determine the bit-error ratio (BER) performance of LDPC-coded on-off keying (OOK) for binary optical coherent state quantum communications. We assume that quantum-receiver is affected by background radiation, and that the phase of a coherent state is either known or random. Secondly, we study the improvements that can be obtained by employing the large-girth structured LDPC codes in $M$-ary phase-shift keying (PSK) optical coherent state quantum communication systems. Both systems are attractive options for deep-space communication, intra-chip/inter-chip optical communications or quantum-key distribution (QKD). Notice that this paper is continuation of our previous papers [10], [11]. In [10] we study the LDPC-coded quantum optical coherent state communication system for OOK and $M$-ary pulse-position modulation with random phase only, while in [11] we describe how to design structured quantum LDPC codes.

The paper is organized as follows. Given the fact that quantum receiver for $M$-ary PSK coherent state communication in the presence of background radiation is not known, in Section II we describe the corresponding receiver in the absence of background radiation. In Section III we describe the binary quantum coherent state communication channel in the presence of background radiation. In Section IV we describe how to calculate the log-likelihood ratios (LLRs), bit-relabilities, required for LDPC decoding. In Section V we describe how to design large girth LDPC codes. In Section VI numerical results are reported. Finally, in last Section some important conclusions are given.

II. $M$-ARY PSK OPTICAL COHERENT STATE QUANTUM COMMUNICATIONS IN THE ABSENCE OF BACKGROUND RADIATION

The received optical field mode is said to be in a coherent state, when the state, described by a ket (vector) $|\alpha\rangle$ (in Dirac notation), is right eigenket of the annihilation operator: $a|\alpha\rangle = \alpha|\alpha\rangle$, with $\alpha$ being a complex eigenvalue. (See [3] and [12] for more details on coherent states, the annihilation operator $a$, the creation operator $a^+$, and the number operator $a^+a$.) The main complications arise because coherent states are not orthogonal. Namely, the coherent state vector $|\alpha\rangle$ can be represented in terms of orthonormal eigenvectors $|n\rangle$ of the number operator $a^+a$ by [3]

$$|\alpha\rangle = \exp[-|\alpha|^2/2] \sum_{n=0}^{+\infty} (n!)^{-1/2} \alpha^n |n\rangle$$

where $|n\rangle$ denotes the number or Fock state. It follows from (1) that the inner product of two coherent states $|\alpha\rangle$ and $|\beta\rangle$, $\langle \alpha | \beta \rangle = \exp[\alpha^* \beta - |\alpha|^2/2 - |\beta|^2/2] \neq 0$, confirming that coherent states are not orthogonal.

If the received optical field for binary coherent state communications, in the absence of background light, is in one pure state $|\psi_0\rangle$ under hypothesis $H_0$ and in another $|\psi_1\rangle$ under hypothesis $H_1$, the corresponding density operators are

$$\rho_0 = |\psi_0\rangle \langle \psi_0|, \quad \rho_1 = |\psi_1\rangle \langle \psi_1|.$$
The transmitted optical field for $M$-ary phase-shift keying (PSK) coherent state quantum communications at every signaling interval $(0, T)$ is represented by one coherent state out of $M$ possible $|\psi_k\rangle \equiv \alpha_k \exp\left[i2\pi(k-1)/M\right]|\langle k | (k = 1, 2, \ldots, M)$, where $\alpha^2 = N_a$ is the average number of photons per symbol. The corresponding received electromagnetic field is specified by one out of $M$ density operators $\rho_1, \ldots, \rho_M$; and the receiver decides among $M$ hypothesis $H_1, \ldots, H_M$, which one $H_j$ corresponds to the transmitted symbol $|\psi_j\rangle$, so that probability of error $P_e$ is minimal. In the absence of background light, the optimum decision strategy is expressed in terms of $M$ projection operators

$$\Pi_k = |w_k\rangle\langle w_k|; \quad k = 1, 2, \ldots, M$$

onto $M$ measurement states (orthogonal axes) $|w_k\rangle$. The location of these axes with respect to the transmitted coherent states should be determined such that the average symbol error probability is minimal. The quantum hypothesis symmetrical set of states case due to Helstrom [3] (see corresponding Section IV.1.d) is directly applicable here. Let us denote the scalar products between transmitted states by $\gamma_{mn} = \langle \psi_m | \psi_n \rangle$, and the components of the $M$ state vectors $|\psi_j\rangle$ along the axes $|w_j\rangle$ by $x_{ij} = \langle w_i | \psi_j \rangle$. Following the procedure due to Helstrom someone can show that minimum $P_e$ is obtained when the components of state vectors along the axes are determined by

$$x_{ik} = M^{-1} \sum_p h_p^{-1/2} \exp[j2\pi(i-k)p/M]$$

where

$$h_p = \sum_{m=1}^{M} \gamma_{m} \exp[-j2\pi(i-m)p/M].$$

The parameter $h_p$ in (5) is in fact the discrete-Fourier transform of $i$th row in correlation matrix $\Gamma = [\gamma_{mn}]$, where $\gamma_{mn}$, as introduced above, is the inner product between transmitted states $|\psi_m\rangle$ and $|\psi_n\rangle$

$$\gamma_{mn} = \langle \psi_m | \psi_n \rangle = \exp[i2\pi(n-m)/M] \langle \psi_m^* | \psi_n \rangle - |\psi_m^*|/\sqrt{2} \neq 0,$$

where for $M$-ary PSK $|\psi_m^*|^2 = N_a$ represents the average number of photons per symbol (that is the same for all symbols), while $\psi_m^* = N_a \exp[i2\pi(n-m)/M]$. Therefore, $\gamma_{mn}$ can be determined by $\gamma_{mn} = \exp[N_a \exp[i2\pi(n-m)/M - 1]]$. The parameters $h_p(p = 1, \ldots, M)$ in (5) represent the eigenvalues of $\Gamma$, which are real and nonnegative because the correlation matrix $\Gamma$ is the circulant Toeplitz matrix (the observed row of the matrix is a right cyclic shift of the row above) [20, 21], and can be efficiently calculated using the fast-Fourier transform (FFT) of arbitrary row in $\Gamma$. The minimum average probability of error in deciding among $M$ hypotheses about the transmitted state $|\psi_m\rangle$ of the system can be determined by [3]

$$P_e = 1 - M^{-1} \left( \sum_p h_p^{-1/2} \right)^2.$$
phase, \( \langle n | \rho_1 | m \rangle = 0(n \neq m) \). The optimum decision strategy would be the measurement of operator \( \rho_1 - \Lambda_0 | 0 \rangle \langle 0 | \) (upon diagonalization) to determine its eigenvalue. Whenever the measured eigenvalue is positive we decide in favor of \( H_1 \), otherwise we decide in favor of \( H_0 \), so that the decision rule can be described as follows:

\[
\eta_k = \frac{P^{(1)}_k - \Lambda_0 P^{(0)}_k}{H_1} > 0 \iff \frac{P^{(1)}_k}{P^{(0)}_k} > \Lambda_0 \quad (10)
\]

where \( P^{(0)}_k = (1 - v)\rho_k \) and \( P^{(1)}_k \) as obtained from

\[\rho_1 = \sum_k P^{(1)}_k | \eta_k \rangle \langle \eta_k | \]

upon diagonalization. Notice that (10) represents the maximum a posteriori probability (MAP) rule.

In next Section, we describe how to calculate the log-likelihood ratios (LLRs), the bit reliabilities, required for LDPC decoding.

IV. DETERMINATION OF LLRS FOR LDPC DECODING

The LLR in random phase OOK case (assuming equal probable transmission, \( \zeta = 1/2 \)) can be determined by

\[
L(\alpha_k) = (1 - v)N_s - \log[L_k(-{(1 - v)^2}N_s/v)],
\]

\[
v = N/(N + 1)
\]

where \( N \) is the average number of noise photons, \( N_s \) is the average number of signal photons, \( L_k \) is the Laguerre polynomial, and \( | \alpha_k \rangle \) represents the \( k \)th coherent state.

It has been shown by Calderbank, Shor and Steane (see [1] and references therein) that good quantum error control coding exist, however, they are quite difficult to implement in quantum domain [1]. On the other hand, we have the option to perform encoding and decoding in “classical electrical” domain and observe the quantum channel as the binary symmetric channel (BSC) with transition probability determined by quantum bit-error ratio (BER). In such a case, the strongest known classical codes—LDPC codes [6]–[8] can be employed. Given the fact that quantum receiver for \( M \)-ary PSK is difficult to implement in quantum domain, this approach represent a reasonable option suitable for application in deep-space optical communications. The LLRs required for soft-iterative LDPC decoding for \( M \)-ary PSK case can be determined by

\[
L(c_k) = (-1)^{c_k} \log \left( \frac{1 - \text{BER}}{\text{BER}} \right)
\]

where \( c_k \) is the quantum hard-decision estimate of \( \hat{c} \)th transmitted bit \( c_k \). Notice that BER of BSC is similar to the shared key BER in the BB84 protocol over the noisy channel.

We turn our attention now to the design of large girth LDPC codes.

V. LARGE GIRTH QUASI-CYCLIC LDPC CODES

The parity check-matrix \( H \) of quasi-cyclic LDPC codes [6]–[8] considered in this paper can be represented by (12), shown at the bottom of the page, where \( I \) is \( p \times p \) (\( p \) is a prime number) identity matrix, \( P \) is \( p \times p \) permutation matrix \((P_{k,i+1} = P_{p,i} = 1, i = 1, 2, \ldots, p - 1 \); other elements of \( P \) are zeros), while \( r \) and \( c \) represent the number of rows and columns in (12), respectively. The set of integers \( S \) are to be carefully chosen from the set \{0, 1, \ldots, \( p - 1 \} \) so that the cycles of short length, in corresponding Tanner (bipartite) graph representation of (12) are avoided. We have shown in [8] that large girth (the shortest cycle in bipartite graph), \( g \geq 10 \), LDPC codes provide excellent improvement in coding gain over corresponding turbo-product codes (TPCs). At the same time complexity of LDPC codes is lower than that of TPCs, selecting them as excellent candidates for application to quantum optical coherent state communications. Moreover, the large girth LDPC codes do not exhibit error floor down to BER of \( 10^{-15} \) [19]. For example, by selecting \( p = 1123 \) and \( S = \{0, 2, 5, 13, 20, 37, 58, 91, 135, 160, 220, 292, 354, 712, 830\} \) an LDPC code of rate 0.8, girth \( g = 10 \), column weight 3 and length \( N = 16845 \) is obtained.

The results of simulations for an additive white Gaussian noise (AWGN) channel model are given in Fig. 1, where we compare the girth-10 quasi-cyclic LDPC codes against RS, concatenated RS, turbo-product, and girth-8 LDPC codes. (Notice that \( Q \)-factor is expressed in dB scale.) The results of simulations are obtained for 30 iterations in sum-product-with-correction-term algorithm [14]. The girth-10 LDPC(24015, 19212) code of rate 0.8 outperforms the concatenation RS(255, 230) + RS(255, 223) (of rate 0.82) by 3.35 dB, and RS(255, 239) by 4.75 dB, both at BER of \( 10^{-7} \). At BER of \( 10^{-10} \) it outperforms lattice based LDPC(8547, 6922) of rate 0.81 and girth-8 by 0.44 dB, and BCH(128, 113) × BCH(256, 239) TPC of rate 0.82 by 0.95 dB. The net effective coding gain at BER of \( 10^{-12} \) is 10.95 dB.

Given the description of quantum and quasi-quantum receivers, and description of large girth LDPC codes suitable for use in quantum communications, in next Section we provide important numerical results.

\[
H = \begin{bmatrix}
    I & I & I & \cdots & I \\
    I & P^{s[1]} & P^{s[2]} & \cdots & P^{s[r-1]} \\
    I & P^{s[1]} & P^{s[2]} & \cdots & P^{s[r-1]} \\
    \vdots & \ddots & \ddots & \ddots & \vdots \\
    I & P^{s[r-1]} & P^{s[r-1]} & \cdots & P^{s[r-1]}
\end{bmatrix}
\]

(12)
VI. NUMERICAL RESULTS

The uncoded probability of symbol error for different sizes of $M$-ary PSK “signal constellation” is shown in Fig. 2 against the average number of photons per bit $S$, which is related to the average number of photons per symbol (coherent state) by $S = N_p / \log_2 M$. The binary OOK coherent state case is also shown for comparison purpose. The BPSK and QPSK perform comparable, while 8-PSK is slightly worse than OOK. 16-PSK performs significantly worse than other cases.

The results of simulations for two different classes of large girth LDPC codes, the lattice codes [6] and quasi-cyclic codes described in Section V, are shown in Fig. 3. For example, to achieve the BER of $10^{-6}$ by using the LDPC(24015, 19212) code of code rate 0.8, column weight of parity-check matrix $w_c = 3$, and girth $g = 10$; the required number of photons is 0.73 for BPSK and 1.42 for OOK. The net-effective coding gain (observed at BER of $10^{-6}$) for the same LDPC code is 7.63 dB for BPSK, and 7.78 dB for OOK. (The larger coding gains are expected at lower BERs.)

The uncoded OOK probability of error, with known and random phases (in the presence of background radiation), is shown in Fig. 4 for different average thermal noise photons values. It is interesting to notice that for small $N$ and large $N$ the differences between those two cases are much smaller than those for intermediate values of $N$. In case when LDPC codes with threshold BER around $10^{-2}$ are employed, we are not getting that much by preserving the phase information between transmitter and receiver, for OOK modulation format.

The results of simulations for LDPC-coded OOK optical coherent state quantum communications in the presence of background light, and assuming that the phase is random are given in Fig. 5. Girth-8 LDPC(8547, 6922) code of code rate 0.81, designed as we explained in [6], is employed in simulations. The required number of signal photons to achieve the BER of $10^{-6}$, for average number of noise photons $N = 0.1$, is three. In the absence of thermal radiation, the required number of signal photons is two. The net effective coding for $N = 0$ is 5.2 dB, and
for $N = 0.1$ is 6.35 dB. The net effective coding gain grows as the average number of noise photons increases.

VII. CONCLUSION

In this paper we consider: 1) the coded $M$-ary PSK optical coherent state quantum communication in the absence of background radiation, and 2) the coded binary OOK optical coherent state quantum communication in the presence of background radiation. In both cases quasi-cyclic high-rate large girth LDPC codes are used. The coherent state quantum communication receiver can be implemented in a fashion similar to the coherent state discrimination by the quantum-feedback [2], [4].

In binary quantum coherent state communication, for the average number of noise photons tending to zero, the BER performance loss due to random phase is negligible, but significant for medium values of $N$. The net effective coding gain (in random phase case) is 6.35 dB at BER of $10^{-6}$, and grows as the number of noise photons increases. To achieve BER around $10^{-6}$ the required number of signal photons is 2 for $N = 0$ and 3 for $N = 0.1$. In the absence of background radiation, the net-effective coding gain (at BER of $10^{-8}$) for the same LDPC code is 7.63 dB for BPSK, and 7.78 dB for OOK.

The possible applications of LDPC-coded coherent state quantum communication systems considered in this paper include deep-space optical communications, inter-chip and intra-chip free-space optical links, and quantum cryptography. For example, the quantum LDPC codes [11] are compatible to modified Lo-Chau QKD protocol via Calderbank-Shor-Steane (CSS) codes [1]. By using the best known codes-LDPC codes (having the error-correction capability $t$), we can increase the number of positions $t$ in which qubits differ before aborting the QKD protocol. For this application, however, the LDPC encoder and decoder have to be implemented in quantum domain as explained in [15]. The ever-increasing demands in miniaturization of electronics on a chip will lead us to the point when for intra-chip/inter-chip communication quantum effects become important and have to be taken into account.

The use of LDPC codes in quantum coherent state communication is proposed because the LDPC codes perform very well for variety channels including wireless channel [16], free-space optical channel [17] and fiber-optics channel in the presence of intra-channel nonlinearities, residual chromatic dispersion and PMD [18]. Moreover, as the level of channel degradation grows the coding gain by LDPC codes is getting larger compared to conventional codes [17], [18]. This suggests that in the presence of background radiation, for $M$-ary PSK coherent state quantum communications, larger coding gains than that in the absence of background radiation are expected.

REFERENCES


Ivan B. Djordjevic (M’XX) is an Assistant Professor of Electrical and Computer Engineering at the University of Arizona, Tucson.

Prior to this appointment in August 2006, he was with University of Arizona, Tucson; University of the West of England, Bristol, U.K.; University of Bristol, Bristol, U.K.; Tyco Telecommunications, Eatontown, NJ; and National Technical University of Athens, Athens, Greece. His current research interests include optical networks, error control coding, constrained coding, coded modulation, turbo equalization, OFDM applications, and quantum communications. He is author of more than 100 international publications. He presently directs the Optical Communications Systems Laboratory (OCSL) within the ECE Department at the University of Arizona.

Dr. Djordjevic serves as an Associate Editor for Research Letters in Optics and as an Associate Editor for International Journal of Optics.