Mathematics and Engineering Communications Laboratory

Technical Report

Performance of Interleaved Non-Binary Block Codes Over Binary Channels with Memory

H. Al-Lawati, *F. Alajaji*, and *C. Pimentel*

September 2007

*Performance of Interleaved Non-Binary Block Codes Over Binary Channels with Memory**

Haider Al-Lawati, Fady Alajaji and Cecilio Pimentel

Abstract

The performance of Reed-Solomon codes over two classes of binary channels with memory, the queue-based channel (QBC) and the Gilbert-Elliott channel (GEC) is analyzed under the assumption of bounded distance decoding. In particular, we examine two interleaving strategies encountered when dealing with non-binary codes over a binary channel; namely, symbol interleaving and bit interleaving. An analytical proof is given demonstrating that perfect (i.e., with infinite interleaving depth) symbol interleaving results in a better performance compared to perfect bit interleaving for any non-binary block code over either the QBC or the GEC with positive noise correlation coefficient. Next, the effect of imperfect interleaving on the code performance is examined. An enumerative approach is applied to derive some useful analytical expressions pertaining to the calculation of the probability of codeword error (PCE) for the simplest scenario of the QBC which is the additive first-order Markov noise channel. Numerical results for PCE are provided for more general QBC models and the GEC. The performance of imperfect interleaved binary codes with imperfect interleaved non-binary codes is compared and the choice of the interleaving depth to achieve a required performance is discussed for different values of the channel parameters.

Index Terms: Interleaving, Gilbert-Elliott channel, Markov noise channel, queue-based channel, probability of codeword error, Reed-Solomon codes.

*This work was supported in part by NSERC of Canada and CNPq of Brazil. The authors are with the Dept. of Mathematics & Statistics, Queen's University, Kingston, ON K7L 3N6, Canada. Cecilio Pimentel is on leave from the Department of Electronics and Systems, Federal University of Pernambuco, 50711-970, Recife, PE, Brazil (email: cecilio@ufpe.br).

1 Introduction

Burst-error correcting codes are of prime theoretical and practical interest due to the bursty nature of real-world wireless digital communication channels. An important class of non-binary burst-error correcting codes used widely in data transmission and storage systems is the family of Reed-Solomon (RS) codes (e.g., [1,2]). A commonly used strategy to enhance the overall burst-correcting capability of a code is to incorporate block interleaving into the communication system. When non-binary codes are sent over a stationary binary additive noise channel with memory, two interleaving strategies are worth considering: interleaving the code (or channel) bits which reduces the channel to the memoryless binary symmetric channel (BSC) (under perfect or infinite interleaving depth) [3] and interleaving the code symbols.

The performance of non-interleaved RS codes on correlated fading channels is analyzed in [4–7] using a two-step procedure. First, a channel model is introduced for the generation of the bit or symbol error process, and then a formula for the probability of codeword error (PCE) under bounded distance decoding is derived for the proposed model. In [4], the channel is modeled via the Gilbert-Elliott channel (GEC) [3] whose parameters are calculated using a simple threshold model. An approximation to the PCE is derived under the assumption that the channel state does not change during each symbol transmission. In [5], level crossing statistics are applied to characterize the fading arrival process and the fading durations, and the PCE is expressed in terms of the probability distribution of the fading durations. In [6], the bit error process resulting from the hard-decision demodulation of binary frequency-shift keying modulated signals over correlated Rician fading channels is modeled via a Fritchman channel. Furthermore, an analytical method based on the generating series approach for calculating the PCE of RS codes over finite state channels is presented. In [7], an L-state Markov chain is proposed to characterize the correlation of symbol errors. Imperfect (finite-length) symbol interleaving is also considered in [5, 6].

This work is concerned about the performance of RS codes (under bounded-distance decoding) over two classes of finite state channels: the GEC (which has been widely shown to be a good model for flat fading channels [8,9]) and the queue-based channel (QBC). The QBC was recently introduced in [10] to model an Mth-order additive Markov noise channel using a finite queue. The QBC has the distinguished feature of having only four parameters (like the GEC), while allowing its memory order to be arbitrarily large. It also offers (unlike the GEC) closed form expressions for the block transition probability, capacity and autocorrelation function [10]. Furthermore, it has been shown that the QBC can accurately approximate the GEC [10] as well as a hard-decision demodulated Rician flat-fading channel [11,12]. We first prove analytically that under bounded-distance decoding, perfect symbol interleaving results in lower PCE compared to perfect bit interleaving for any non-binary block code over either the QBC or the GEC with positive noise correlation coefficient. A

numerical study of the superiority of symbol-interleaved RS codes is given in [13] for the case of slow fading channels, but there is no analytical proof of this result. Interestingly, we note an opposite behavior for first-order Markov noise channels when the noise correlation coefficient is negative (this channel is a special instance of the GEC); in this case, we show that bit-interleaved non-binary codes outperform symbol-interleaved ones. Next, we examine the effect of imperfect (i.e., with finite interleaving depth) symbol interleaving on the performance of RS codes over the QBC and the GEC. Using the generating series approach of [6] we derive a useful analytical expression for the probability of m symbol errors in a block of n symbols, $P(m, n)$, for imperfect symbol-interleaved non-binary codes for the QBC with memory $M = 1$, i.e., for the additive first-order Markov noise channel with non-negative noise correlation coefficient. This simple (memory-one) model has been used to characterize correlated fading channels at the packet level [14,15]. A simpler recursion than the one derived in [16] for binary codes is obtained. Finally, we provide PCE numerical results when imperfect symbol-interleaved RS codes are sent over either the QBC with $M > 1$ or the GEC. We compare different coding schemes under the same interleaving memory requirement and discuss the choice of the interleaving depth to achieve a required performance.

The rest of this paper is organized into four sections. Preliminaries on the channel models are provided in Section 2. Section 3 compares the performance of non-binary codes under perfect bit and perfect symbol interleaving when transmitted over either the QBC or the GEC. The coding performance under imperfect interleaving is analyzed in Section 4. Conclusions are presented in Section 5.

2 System Description

We consider a coded communication system where non-binary transmitted symbols, assuming values from the Galois field GF(2^b), are mapped one-to-one to a binary b-tuple and are transmitted across a binary channel. The kth received binary symbol Y_k is described by $Y_k = X_k \oplus Z_k$, $k = 1, 2, \cdots$, where $\oplus$ denotes addition modulo-2, $X_k \in \{0, 1\}$ is the kth transmitted symbol and $Z_k \in \{0, 1\}$ is the kth channel noise symbol. We assume that the noise process is stationary and is independent of the transmitted symbols. Two channel models considered in this work are described as follows.

2.1 Queue-Based Channel

The queue-based channel (QBC) uses a simple approach to model an Mth-order Markov noise process via a finite queue [10]. At the kth time, the channel generates a noise output Z_k that depends on four parameters: The size of the queue, M, the channel bit error rate (BER), $p = \Pr(Z_k = 1)$,

and correlation parameters ε and α, where $0 \leq \varepsilon < 1$, $\alpha \geq 0$. The channel state process $\{S_k\}_{k=-\infty}^{\infty}$, where $S_k \triangleq (Z_k, Z_{k-1}, \cdots, Z_{k-M+1})$ is a homogeneous first-order Markov process with an alphabet of size 2^M. The (i,j)th entry of the state transition probability matrix, denoted by $\mathbf{P} = [p_{ij}]$, where p_{ij} denotes the conditional probability that $S_k = j$ given that $S_{k-1} = i$, is given by

$$p_{ij} = \begin{cases} \left(M - \omega_i^{(M)} - 1 + \alpha\right) \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p), & \text{if } j = \frac{i}{2}, \text{ and } i \text{ is even} \\ \left(M - \omega_i^{(M)}\right) \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p), & \text{if } j = \lfloor \frac{i}{2} \rfloor, \text{ and } i \text{ is odd} \\ \omega_i^{(M)} \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p, & \text{if } j = \frac{i+2^M}{2}, \text{ and } i \text{ is even} \\ \left(\omega_i^{(M)} - 1 + \alpha\right) \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p, & \text{if } j = \lfloor \frac{i+2^M}{2} \rfloor, \text{ and } i \text{ is odd} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where $i, j = 0, 1, \cdots, 2^M - 1$ and $\omega_i^{(M)}$ is the number of "ones" in the M-bit binary representation of the decimal integer i. The ith component of the state stationary distribution column vector $\mathbf{\Pi} = [\pi_i]$ is given by [10]

$$\pi_i = \frac{\prod_{j=0}^{M-1-\omega_i^{(M)}} \left[j \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)\right] \prod_{j=0}^{\omega_i^{(M)}-1} \left[j \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p\right]}{\prod_{j=0}^{M-1} \left[1 - (\alpha + j) \frac{\varepsilon}{M-1+\alpha}\right]}. \tag{2}$$

We define two $2^M \times 2^M$ matrices $\mathbf{P}(0)$ and $\mathbf{P}(1)$, $\mathbf{P}(0) + \mathbf{P}(1) = \mathbf{P}$, where the (i,j)th entry of the matrix $\mathbf{P}(z)$, $z \in \{0,1\}$ is $\Pr(Z_k = z, S_k = j \mid S_{k-1} = i)$. For the QBC, the first 2^{M-1} columns of $\mathbf{P}(0)$ are exactly the same as those of $\mathbf{P}$, while the remaining 2^{M-1} columns are zeros. Similarly, the first 2^{M-1} columns of $\mathbf{P}(1)$ are all zeros, while the remaining 2^{M-1} columns are exactly the same as those of $\mathbf{P}$.

The QBC allows simple closed-form expressions for several statistics. In particular, the channel noise block probability $\Pr(Y^n = y^n | X^n = x^n) = \Pr(Z^n = z^n)$ is expressed as [10]

- For blocklength $n \leq M$,

$$\Pr(Z^n = z^n) = \frac{\prod_{j=0}^{n-d_1^n-1} \left[j \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)\right] \prod_{j=0}^{d_1^n-1} \left[j \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p\right]}{\prod_{j=M-n}^{M-1} \left[1 - (\alpha + j) \frac{\varepsilon}{M-1+\alpha}\right]} \tag{3}$$

  where $d_a^b = z_b + z_{b-1} + \cdots + z_a$ ($d_a^b = 0$ if $a > b$), and $\prod_{j=0}^{a}(\cdot) \triangleq 1$ if $a < 0$.

- For blocklength $n \geq M + 1$,

$$\Pr(Z^n = z^n) = L^{(M)} \prod_{i=M+1}^{n} \left[\left(d_{i-M+1}^{i-1} + \alpha z_{i-M}\right) \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p\right]^{z_i}$$
$$\left\{\left[\left(M - 1 - d_{i-M+1}^{i-1}\right) + \alpha(1 - z_{i-M})\right] \frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)\right\}^{1-z_i} \tag{4}$$

where

$$L^{(M)} = \frac{\prod_{j=0}^{M-1-d_1^M} \left[j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p) \right] \prod_{j=0}^{d_1^M-1} \left[j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)p \right]}{\prod_{j=0}^{M-1} \left[1 - (\alpha+j)\frac{\varepsilon}{M-1+\alpha} \right]}.$$

The noise correlation coefficient, Cor, for the QBC is a non-negative quantity given by

$$\text{Cor} = \frac{\frac{\varepsilon}{M-1+\alpha}}{1-(M-2+\alpha)\frac{\varepsilon}{M-1+\alpha}}. \tag{5}$$

A special case of the QBC is the binary additive Markov noise channel (BAMNC) with non-negative correlation coefficient. In this case, the BAMNC is equivalent to the QBC with $M = \alpha = 1$ and correlation coefficient ε. As a result, the BAMNC is a two-state first-order Markov noise channel with stationary distribution vector $\mathbf{\Pi} = [1-p, p]^T$ (the superscript $[\cdot]^T$ indicates the transpose of a matrix) and transition probability matrix $\mathbf{P} = \mathbf{P}(0) + \mathbf{P}(1)$ where

$$\mathbf{P}(0) = \begin{bmatrix} \varepsilon + (1-\varepsilon)(1-p) & 0 \\ (1-\varepsilon)(1-p) & 0 \end{bmatrix} \tag{6}$$

$$\mathbf{P}(1) = \begin{bmatrix} 0 & (1-\varepsilon)p \\ 0 & \varepsilon + (1-\varepsilon)p \end{bmatrix}. \tag{7}$$

When $\varepsilon = 0$ (Cor $= 0$), the noise process becomes independent and identically distributed and the resulting model reduces to the memoryless BSC with crossover probability p.

2.2 Gilbert-Elliott Channel

The Gilbert-Elliott channel (GEC) is driven by an underlying stationary ergodic two-state Markov chain composed of state 0, which produces errors with probability p_G, and state 1, where errors occur with probability p_B, where $p_G < p_B$. The transition probabilities of the Markov chain are $p_{01} = Q$ and $p_{10} = q$, where $0 < Q < 1$ and $0 < q < 1$. Mushkin and Bar-David [3] defined the "memory" of the Gilbert-Elliott channel as $\mu = 1 - q - Q$. If $\mu > 0$ the channel has persistent memory, or if $\mu < 0$ the channel has oscillatory memory [3]. When $\mu = 0$ the model reduces to the memoryless BSC. The state stationary distribution vector $\mathbf{\Pi}$, and the matrices $\mathbf{P}(0)$ and $\mathbf{P}(1)$ are given by

$$\mathbf{\Pi} = \begin{bmatrix} \pi_0 \\ \pi_1 \end{bmatrix} = \begin{bmatrix} \frac{q}{q+Q} \\ \frac{Q}{q+Q} \end{bmatrix} = \begin{bmatrix} \frac{\rho}{1+\rho} \\ \frac{1}{1+\rho} \end{bmatrix} \tag{8}$$

$$\mathbf{P}(0) = \begin{bmatrix} (1-Q)(1-p_G) & Q(1-p_B) \\ q(1-p_G) & (1-q)(1-p_B) \end{bmatrix} \tag{9}$$

$$\mathbf{P}(1) = \begin{bmatrix} (1-Q)\,p_G & Q\,p_B \\ q\,p_G & (1-q)\,p_B \end{bmatrix} \tag{10}$$

respectively, where $\rho = q/Q$. The channel noise block probability can be expressed in matrix form as

$$\Pr(Z^n = z^n) = \boldsymbol{\Pi}^T \left(\prod_{k=1}^{n} \mathbf{P}(z_k) \right) \mathbf{1} \tag{11}$$

where $\mathbf{1}$ is a column vector of ones of length 2.

Example 1 *The probability of a correct transmission,* $p_0 \triangleq \Pr(Z_k = 0)$*, and the probability of two consecutive zeros,* $p_{00} \triangleq \Pr(Z_k = 0, Z_{k+1} = 0)$ *for the GEC are given by*

$$p_0 = 1 - BER = \pi_0(1-p_G) + \pi_1(1-p_B) \tag{12}$$

$$p_{00} = \pi_0(1-Q)(1-p_G)^2 + 2\pi_0 Q(1-p_G)(1-p_B) + \pi_1(1-q)(1-p_B)^2. \tag{13}$$

The noise correlation coefficient for the GEC is expressed as

$$\text{Cor} = \frac{\mu(\text{BER} - p_G)(p_B - \text{BER})}{\text{BER}(1-\text{BER})} = \frac{\mu(p_B - p_G)^2\rho}{(\rho\,p_G + p_B)\,(1 + \rho(1-p_G) - p_B)}. \tag{14}$$

The BAMNC can be obtained from the GEC by setting $p_G = 0$ and $p_B = 1$. In this work, we only consider a GEC with $\mu \geq 0$ (or $\text{Cor} \geq 0$) due to its relevance in modeling fading channels. [1]

3 Comparison Between Perfect Bit and Perfect Symbol Interleaving under Non-binary Coding

The objective of this section is to analytically compare the performance of non-binary codes under both perfect symbol interleaving and perfect bit interleaving when transmitted over either the QBC or the GEC.

Let $\mathcal{C}$ be any non-binary linear block code over the Galois field $\text{GF}(2^b)$ with length n and error correction capability t (e.g., a Reed-Solomon code). A transmitted symbol is received correctly if

[1] We modeled a discrete channel that employs a binary frequency-shift keying modulation, a Rician fading channel with Clarke's autocorrelation function, and a hard quantized non-coherent demodulation using the GEC (as in [12]). For the range of fading parameters that yields a GEC with negative memory, we observed no significant gain in capacity of the GEC over the BSC. For example, for a discrete channel with signal-to-noise ratio 8 dB, normalized Doppler frequency ($f_D T$) 0.6 dB and Rician factor 3 dB, we obtained a GEC with parameters $p_G = 0.017$, $p_B = 0.17$, $q = 0.813$, $Q = 0.695$. The resulting $\text{BER} = 0.0875$, $\mu = -0.508$ and the capacity of the BSC and GEC is, respectively, 0.572 and 0.573. For the case of Rayleigh fading, the correlation coefficient of this discrete channel is always non-negative.

the noise corrupting it is a sequence of zeros of length b, denoted as 0^b. Otherwise, the transmitted symbol is received incorrectly and a symbol error occurs. Let the probability that the channel produces the b-tuple all zeros be denoted by $F(b) = \Pr(Z^b = 0^b)$. Then the probability of correct decoding under bounded distance decoding, denoted P_c, for the perfect symbol-interleaved system is given by

$$P_c = \sum_{i=0}^{t} \binom{n}{i} (1 - F(b))^i (F(b))^{n-i}. \tag{15}$$

On the other hand, for the perfect bit-interleaved non-binary code, denote the probability of correct b transmissions by $G(b) \triangleq \Pr(Z = 0)^b$. Hence the probability of correct decoding for this interleaving scheme is given by (15) with replacing $F(b)$ by $G(b)$. The performance comparison carried out in this section is done in terms of P_c, or equivalently, in terms of PCE $= 1 - P_c$.

Lemma 1 *If $F(b) > G(b)$, then perfect symbol interleaving outperforms perfect bit interleaving for the transmission of $\mathcal{C}$ under bounded distance decoding.*

Proof: Define the functions $f(x)$ and $g(x)$ for $x \in [0, n]$ as follows

$$\begin{aligned} f(x) &= (1 - F(b))^x (F(b))^{n-x} \\ g(x) &= (1 - G(b))^x (G(b))^{n-x}. \end{aligned}$$

If $F(b) > G(b)$, then $f(0) > g(0)$ and $f(n) < g(n)$ and hence $f(x)$ and $g(x)$ have at least one point of intersection. However, $\ln(f(x))$ and $\ln(g(x))$ are both linear functions in x, which means that they have at most one point of intersection. Therefore, $f(x)$ and $g(x)$ have a unique point of intersection obtained by solving the equation $f(x) = g(x)$. In particular, letting this point of intersection be x_0, we obtain that

$$x_0 = n \frac{\ln(G(b)/F(b))}{\ln((1 - F(b))/F(b)) + \ln(G(b)/(1 - G(b)))}.$$

Furthermore, $f(x) > g(x)$ if $x < x_0$ and $f(x) < g(x)$ otherwise. Since t is an integer between 0 and n, we first assume that $t \leq x_0$. Thus

$$\sum_{i=0}^{t} \binom{n}{i} (1 - F(b))^i (F(b))^{n-i} > \sum_{i=0}^{t} \binom{n}{i} (1 - G(b))^i (G(b))^{n-i}. \tag{16}$$

In other words, the probability of correct decoding for the symbol-interleaved system is greater than the probability of correct decoding for the bit-interleaved one. Now assume that $t > x_0$; then

$$\sum_{i=t+1}^{n} \binom{n}{i} (1 - F(b))^i (F(b))^{n-i} < \sum_{i=t+1}^{n} \binom{n}{i} (1 - G(b))^i (G(b))^{n-i}. \tag{17}$$

The relation (17) states that symbol interleaving achieves a lower PCE compared to bit interleaving. ■

In light of Lemma 1, we next show that perfect symbol interleaving is always better compared to perfect bit interleaving when the non-binary code is transmitted over either the QBC or the GEC with positive memory.

Proposition 1 *Under bounded distance decoding, perfect symbol interleaving outperforms perfect bit interleaving when non-binary codes over GF(2^b) are transmitted over the QBC, for $\varepsilon > 0$ and $p > 0$.*

Proof: From Lemma 1, it is enough to show that $F(b) > G(b)$ for the QBC. For this channel, $G(b) = (1-p)^b$ and for $b \leq M$ we express $F(b)$ using (3) as

$$F(b) = \prod_{j=0}^{b-1} \frac{j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}}. \tag{18}$$

For each $j > 0$ we notice that for $p > 0$,

$$\frac{j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}} > (1-p). \tag{19}$$

Because $b > 1$ (for non-binary codes), we get

$$\prod_{j=0}^{b-1} \frac{j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}} > (1-p)^b \tag{20}$$

which implies that $F(b) > G(b)$. When $b > M$, $F(b)$ is expressed using (4) as

$$F(b) = \prod_{j=0}^{M-1} \frac{j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}} (\varepsilon + (1-\varepsilon)(1-p))^{b-M}. \tag{21}$$

We already remarked that $\frac{j\frac{\varepsilon}{M-1+\alpha}+(1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}} > (1-p)$ for $j > 0$. We also note that

$$\varepsilon + (1-\varepsilon)(1-p) = (1-p) + \varepsilon p \geq (1-p)$$

with equality if and only if either $p = 0$ or $\varepsilon = 0$. Therefore, we combine the above two inequalities to get that

$$\left(\prod_{j=0}^{M-1} \frac{j\frac{\varepsilon}{M-1+\alpha} + (1-\varepsilon)(1-p)}{1-(\alpha+M-1-j)\frac{\varepsilon}{M-1+\alpha}} (\varepsilon + (1-\varepsilon)(1-p))^{b-M} \right) > (1-p)^M (1-p)^{b-M} = (1-p)^b.$$

Therefore $F(b) > G(b)$ (the inequality is strict because we assume that both p and $\varepsilon \neq 0$). ■

We now consider the GEC model. In this case, $G(b) = (1 - p_0)^b$, where an expression for p_0 is given in Example 1. We do not derive an explicit expression for $F(b)$. Alternatively, we define the generating series for $F(b)$ as

$$F(z) \triangleq \sum_{b=0}^{\infty} F(b) z^b. \tag{22}$$

It follows from (11) that $F(b) = \boldsymbol{\Pi}^T \mathbf{P}^b(0)\mathbf{1}$. Then [17]

$$F(z) = \boldsymbol{\Pi}^T (\mathbf{I} - \mathbf{P}(0)z)^{-1}\mathbf{1} \tag{23}$$

where $\mathbf{I}$ is the identity matrix. For the GEC, $F(z)$ in (23) becomes

$$F(z) = \frac{1 + a_1 z}{1 + b_1 z + b_2 z^2} \tag{24}$$

where

$$a_1 = -\mu \left[\pi_1(1 - p_G) + \pi_0(1 - p_B)\right] \tag{25}$$

$$b_1 = -[(1 - \mu)p_0 + \mu(2 - p_G - p_B)] \tag{26}$$

$$b_2 = \mu\,(1 - p_G)(1 - p_B). \tag{27}$$

The following recursion formula is derived directly from (24)

$$F(b) = -b_1 F(b - 1) - b_2 F(b - 2) \tag{28}$$

for $b \geq 2$, with initial conditions $F(0) = 1$ and $F(1) = p_0$. The condition stated in Lemma 1 for the GEC follows from the next lemma.

Lemma 2 *The following relation is satisfied for the GEC with* $\mu > 0$

$$\frac{F(b)}{F(b - 1)} > p_0, \quad \textit{for} \;\; b \geq 2. \tag{29}$$

Proof: The proof is by induction on b. For $b = 2$, the expressions in Example 1 yield

$$\frac{F(2)}{F(1)} = \frac{p_{00}}{p_0} = -b_1 - \frac{b_2}{p_0} = p_0 + \mu \frac{\pi_0 \pi_1 (p_B - p_G)^2}{p_0} > p_0 \tag{30}$$

since $\mu > 0$. Next assume that the statement (29) is true for a fixed $b \geq 2$. It follows from (28) that

$$F(b + 1) = -b_1 F(b) - b_2 F(b - 1) \tag{31}$$

or

$$\frac{F(b+1)}{F(b)} = -b_1 - b_2 \frac{F(b-1)}{F(b)}. \tag{32}$$

We conclude from the inductive hypothesis that $F(b-1)/F(b) < 1/p_0$, and since $b_2 > 0$ for $\mu > 0$, we obtain that

$$\frac{F(b+1)}{F(b)} > -b_1 - \frac{b_2}{p_0} = \frac{F(2)}{F(1)} > p_0. \tag{33}$$

■

By using (29) repeatedly for increasing values of b, we obtain a chain of inequalities of the form $F(b) > F(b-x)p_0^x$. In particular, when $x = b$, $F(b) > G(b)$. Thus, we have proved the following proposition.

Proposition 2 *Perfect symbol interleaved transmission of $\mathcal{C}$ performs better than the bit interleaved one over the GEC with $\mu > 0$, assuming bounded distance decoding.*

We next observe that for some classes of models with negative noise correlation coefficient, perfect bit interleaving is surprisingly better than perfect symbol interleaving, but we stress that this is not a general trend. [2]

Remark 1 *Note that in Proposition 1, if $F(b) < G(b)$, then we get the opposite result compared to the positive noise correlation case; i.e., perfect bit interleaving outperforms perfect symbol interleaving. For the BAMNC, $F(b)$ and $G(b)$ are given by*

$$\begin{aligned} F(b) &= \left[(1-p)(\varepsilon + (1-\varepsilon)(1-p))^{b-1}\right] \\ G(b) &= \left[(1-p)^b\right]. \end{aligned}$$

Note that when $\varepsilon < 0$, then $F(b) < G(b)$.

Given a particular non-binary linear code, we next examine the effect of imperfect (symbol or bit) interleaving on the performance of this code over a binary additive-noise channel with memory defined in terms of the matrices $\mathbf{P}(0)$ and $\mathbf{P}(1)$. In this scenario, the symbols within a codeword are corrupted by correlated channel noise symbols and (15) cannot be used in the performance analysis. In the next section, we consider an analytical method based on generating series that expresses the probability of the number of error symbols produced by the interleaved channel in terms of the coefficients in a formal power series [6]. Recursion formulas are derived for the BAMNC to simplify the analysis and numerical results are provided for the QBC (with $M \geq 1$) and GEC.

[2] For example, we can find the parameters of a simplified Fritchman channel [18] with negative noise correlation coefficient with 2 good states and 1 bad state such that $F(2) > G(2)$ but $F(3) < G(3)$. Thus, for this channel, neither perfect symbol interleaving nor perfect bit interleaving is always better, since this comparison depends on the code's field size 2^b.

4 Performance Evaluation under Imperfect Interleaving

Recall that $\mathcal{C}$ is a non-binary linear block code GF(2^b) with length n and an error correction capability of t symbols per codeword. We assume block symbol interleaving with nb columns (codeword length in bits) and I_d (interleaving depth) rows [19]. The symbols are written into the array by rows and read out by columns. The b bits within each symbol are transmitted consecutively through the channel.

The probabilities P_c and PCE are given by

$$P_c = \sum_{m=0}^{t} P(m,n) \quad \text{and} \quad \text{PCE} = 1 - P_c$$

respectively, where $P(m,n)$ is the probability that m symbol errors occur in a block of n symbols. Given indeterminates s and z, define the formal power series $P(s,z) = \sum_{n=0}^{\infty} \sum_{m=0}^{n} P(m,n)\, s^m\, z^n$. Thus $P(m,n)$ can be derived as the coefficient of $s^m z^n$ in $P(s,z)$. For a 2^b-ary code transmitted over a binary imperfect symbol interleaved channel, $P(s,z)$ is given by [6]

$$P(s,z) \triangleq \ \mathbf{\Pi}^T \left[\mathbf{I} - z\{\mathbf{P}(0)^b + s(\mathbf{P}^b - \mathbf{P}(0)^b)\}\mathbf{P}^{(I_d-1)b}\right]^{-1} \mathbf{1}. \tag{34}$$

4.1 Analytical Recursion for $P(m,n)$ over the BAMNC

We specialize (34) for the BAMNC defined by the matrices (6) and (7). For the BAMNC, it can be shown by induction (see [16]) that for any integer n

$$\mathbf{P}^n = \begin{bmatrix} \varepsilon^n + (1-p)(1-\varepsilon^n) & p(1-\varepsilon^n) \\ (1-p)(1-\varepsilon^n) & \varepsilon^n + (1-\varepsilon^n)p \end{bmatrix}.$$

It can also be shown by induction that for any integer n

$$\mathbf{P}(0)^n = \begin{bmatrix} (\varepsilon + (1-p)(1-\varepsilon))^n & 0 \\ (1-\varepsilon)(1-p)(\varepsilon + (1-p)(1-\varepsilon))^{n-1} & 0 \end{bmatrix}.$$

Since $P(s,z)$ in (34) is a ratio of two polynomials, a recursive expression for $P(m,n)$ is obtained by examining the denominator polynomial, which is the determinant of the matrix $\mathbf{I} - z\{\mathbf{P}(0)^b + s(\mathbf{P}^b - \mathbf{P}(0)^b)\}\mathbf{P}^{(I_d-1)b}$. Specifically,

$$\begin{aligned} P(m,n) \ = \ & [\varepsilon + (1-\varepsilon)(1-p)]^{(b-1)}(1 - p + p\varepsilon^{1+b(I_d-1)})\, P(m,n-1) \\ & -[(\varepsilon + (1-\varepsilon)(1-p))^{(b-1)}[1 - p + p\varepsilon^{1+b(I_d-1)}] - (1+\varepsilon^{bI_d})]\, P(m-1,n-1) \\ & -[(\varepsilon + (1-\varepsilon)(1-p))^{b-1}(\varepsilon^b(1-p) + \varepsilon p)]\varepsilon^{b(I_d-1)}\, P(m-1,n-2) \\ & -[\varepsilon^b - (\varepsilon^b(1-p) + p\varepsilon)(\varepsilon + (1-\varepsilon)(1-p))^{b-1}]\varepsilon^{b(I_d-1)}\, P(m-2,n-2) \end{aligned} \tag{35}$$

for $n \geq 2$, with initial conditions given by

$$\begin{aligned} P(m,n) &= 0, \qquad \text{if } m,n<0 \text{ or } m<n \\ P(0,0) &= 1 \\ P(0,1) &= (1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1} \\ P(1,1) &= 1-(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}. \end{aligned}$$

In the following, some special cases of (35) are considered. If $I_d = 1$ (i.e., no interleaving is used), then $P(m,n)$ becomes

$$\begin{aligned} P(m,n) \;=\; & [\varepsilon+(1-\varepsilon)(1-p)]^b\, P(m,n-1) \\ & -[(\varepsilon+(1-\varepsilon)(1-p))^b-(1+\varepsilon^b)]\, P(m-1,n-1) \\ & -[(\varepsilon+(1-\varepsilon)(1-p))^{b-1}(\varepsilon^b(1-p)+\varepsilon p)]\, P(m-1,n-2) \\ & -[\varepsilon^b-(\varepsilon^b(1-p)+p\varepsilon)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}]\, P(m-2,n-2) \end{aligned} \tag{36}$$

with the same initial conditions as above.

If $b = 1$ (i.e., the code is binary), then we have a bit interleaved binary codes, and $P(m,n)$ reduces to

$$\begin{aligned} P(m,n) \;=\; & [1-p(1-\varepsilon^{I_d})]\, P(m,n-1) \;+\; (\varepsilon^{I_d}+(1-\varepsilon^{I_d})p)P(m-1,n-1) \\ & -\varepsilon^{I_d}\, P(m-1,n-2). \end{aligned} \tag{37}$$

This is a simpler expression than the one derived in [16] for the same binary system as it contains one less term.

4.2 Numerical Results

We next validate our analytical derivation of $P(m,n)$ in (35) by comparing the PCE calculated using $P(m,n)$ at different interleaving depths with the PCE obtained via simulations (implemented using the Berlekamp-Massey decoding algorithm). We consider an (n,k) RS code over GF(2^b) with codewords of length n and k information symbols. The rate of the code is $R = k/n$, and the code can correct up to $t = \lfloor (n-k)/2 \rfloor$ symbols (under bounded distance decoding).

Fig. 1 shows a typical PCE versus p for the symbol interleaved (127,65) RS code ($b = 7$, $t = 31$ symbols) over the BAMNC with $\varepsilon = 0.8$, for $I_d = 1, 2, 10000$. The curves in this figure indicate a complete agreement between the simulations and the numerical calculations (a similar behavior is observed for other RS codes). Thus (35) provides an effective tool for determining PCE without the need for simulations which can be complex and time-consuming when targeting small PCE values.

Given a QBC with $M \geq 1$ or a GEC with matrices $\mathbf{P}(0)$ or $\mathbf{P}(1)$, we do not establish an explicit analytical recursion for $P(m,n)$ since in these cases, $P(m,n)$ would have a significantly more tedious expression than (35). Instead, for specific model parameters, we apply (34) to derive a recursion with numerical coefficients. The comparison between simulations and numerical calculations is shown in Fig. 2 where curves of PCE versus p are plotted for the symbol-interleaved (127,65) RS code over the QBC model with parameters $M = 3$, $\varepsilon = 0.92$ and $\alpha = 1$ (Cor = 0.8), and for three values of I_d. The accuracy of the recursion is also observed in this figure.

Fig. 3 presents PCE versus I_d for a symbol interleaved shortened (73,57) RS code (with $R = 0.78$, $b = 7$, $t = 8$ symbols) over the GEC. The parameters of the GEC are $\mu = 0.9$, BER $= 0.007$, $p_G = 0.001$ and three values of $\rho = q/Q$, $\rho = 60, 100, 150$ are used. For these values of ρ, the noise correlation coefficients are, respectively, 0.28, 0.46, 0.7. For comparison purposes, we also show curves for the bit interleaved binary (511, 394) BCH code (with $R = 0.77$, $b = 1$, $t = 13$). The coding parameters are selected such that all codes have roughly the same length (in bits) and code rate. Therefore, the memory requirement for interleaving, $b\,n\,I_d$ bits, is the same for each code. We remark that comparison between these two codes is strongly dependent upon a particular value of I_d and ρ. For small values of ρ ($\rho < 60$ in the figure) the perfect (under $I_d \geq 50$) bit-interleaved binary BCH code is more efficient than the perfect (under $I_d \geq 10$) symbol-interleaved RS code, because the erroneous bits are evenly distributed over the received word. On the other hand, longer bursts help the performance of RS decoders, since the error bits become more concentrated and affects fewer symbols in a codeword. We observe that the RS code outperforms the BCH code when I_d is small. In particular, in situations where the maximum value of I_d is limited or when the channel has long bursts, the performance of RS codes stands out. The range of values of ρ where the RS code outperforms the BCH code becomes larger as the BER increases, as is shown in Fig. 4.

From Figs. 3 and 4, we observe that perfect-symbol interleaving is achieved for the RS codes with $I_d = 10$, while for the BCH codes perfect-bit interleaving is achieved with $I_d = 50$. We denote this value of I_d that renders the channel block memoryless by $I_d^\star$. These values of $I_d^\star$ found from the figures are insensitive to the noise correlation coefficient of the channel. For the parameters of the GEC considered in Figs. 3 and 4, the average burst length, $\lambda = 1/q$, is approximately equal to 10.1. Thus, we notice a linear relationship between λ and $I_d^\star$, which is expressed as $I_d^\star = \lambda$ for the RS code and $I_d^\star = 5\,\lambda$ for the BCH code. This relationship is verified in Fig. 5 where the parameters of the GEC are $\mu = 0.95$, BER $= 0.007$, $p_G = 0.001$ and $\rho = q/Q$, with $\rho = 60, 100, 150$. The value of λ is approximately 20.2 and we remark from the figure that $I_d^\star = 20$ for the RS code and $I_d^\star = 100$ for the BCH code.

Finally, Fig. 6 compares the performance of the (73,57) RS code under imperfect bit and symbol interleaving over the GEC with parameters $\mu = 0.9$, BER=0.007, $p_G = 0.001$ and $\rho = 60, 100, 150$.

For this channel with positive noise correlation coefficient, we observe that symbol interleaving outperforms bit interleaving for all values of I_d. Thus, this figure provides numerical evidence that Proposition 2 is also valid for imperfect interleaving.

5 Conclusions

We studied the performance of interleaved linear block codes (under bounded distance decoding) over the QBC and the GEC with positive noise correlation coefficient, which are good models for discretized fading channels. We first proved that when using non-binary block codes over these channels, perfect bit interleaving at the (code) symbol level always outperforms interleaving at the (code) bit level. This result was also illustrated numerically for finite-depth interleaving. The numerical plots presented for PCE under finite interleaving were generated by first deriving recurrence formulas from the matrix expressions for the generating series of the probability $P(m, n)$, which is the probability that m symbol errors occur in a block of n symbols. We observed that for certain channel conditions, it is advantageous to employ a binary BCH code together with bit interleaving as opposed to a non-binary RS code with symbol interleaving. For the GEC, we also observed that perfect interleaving is realized when the interleaved depth is a multiple of the average burst length. The investigation whether this result is valid for other channel model and the determination of the proportionality factor between λ and $I_d^\star$ is an interesting direction for future work. Another worthy direction for future work is the design of an RS decoding technique that judiciously exploit the channel statistical noise memory, thus resulting in potentially substantial performance improvements.

References

[1] J. Roberts, A. Ryley, D. Jones, and D. Burke, "Analysis of error-correction constraints in a optical disk," *Applied Optics,* vol. 35, pp. 3915-3924, July 1996.

[2] H. Chang, C. Shung, and C. Lee, "A Reed-Solomon product-code (RS-PC) decoder chip for DVD applications," *IEEE Journal of Solid-State Circuits,* vol. 36, pp. 229-238, Feb. 2001.

[3] M. Mushkin and I. Bar-David, "Capacity and coding for the Gilbert-Elliott channel," *IEEE Trans. Inform. Theory,* vol. 35, pp. 1277-1290, Nov. 1989.

[4] H. Labiod "Performance of Reed Solomon error-correcting codes on fading channels," in *Proc. IEEE Int. Conf. Personal Wireless Commun.,* 1999, pp. 259-263.

[5] J. Lai and N. Mandayam, "Performance of Reed-Solomon codes for hybrid-ARQ over Rayleigh fading channels under imperfect interleaving," *IEEE Trans. Commun.,* vol. 48, pp. 1650-1659, Oct. 2000.

[6] C. Pimentel and I. F. Blake, "Concatenated coding performance for FSK modulation on time-correlated Rician fading channels," *IEEE Trans. Commun.,* vol. 46, pp. 1610-1618, Dec. 1998.

[7] T. Berman and J. Freedman "Non-interleaved Reed-Solomon coding over a bursty channel," in *Proc. IEEE Military Commun. Conf.,* 1992, pp. 580-583.

[8] L. Wilhelmsson and L. B. Milstein, "On the effect of imperfect interleaving for the Gilbert-Elliott channel," *IEEE Trans. Commun.*, vol. 47, pp. 681-688, May 1999.

[9] C. Pimentel, T. H. Falk, and I. F. Blake, "Finite-state Markov modeling of correlated Rician-fading Channels ," *IEEE Trans. Veh. Technol.*, vol. 53, pp.1491-1501, Sept. 2004.

[10] L. Zhong, F. Alajaji and G. Takahara, "A binary communication channel with memory based on a finite queue," *IEEE Trans. Inform. Theory,* vol. 53, pp. 2815-2840, Aug. 2007.

[11] L. Zhong, F. Alajaji and G. Takahara, "A queue-based model for wireless Rayleigh fading channels with memory," in *Proc. IEEE 62nd Semiannual Veh. Technol. Conf.,* 2005, pp. 1362-1366.

[12] L. Zhong, F. Alajaji and G. Takahara, "A model for correlated Rician fading channels based on a finite queue," *IEEE Trans. Veh. Technol.*, vol. 57, to appear. Jan. 2008.

[13] S. B. Wicker, "Reed-Solomon error control coding for Rayleigh fading channels with feedback," *IEEE Trans. Veh. Technol.*, vol. 41, pp. 124-133, May. 1992.

[14] M. Zorzi, R. Rao, and L. B. Milstein, "ARQ error control for fading mobile radio channels," *IEEE Trans. Veh. Technol.*, vol. 46, pp. 445-455, May 1997.

[15] F. Babich and G. Lombardi, "A Markov model for the mobile propagation channel," *IEEE Trans. Veh. Technol.*, vol. 49, pp. 63-73, Jan. 2000.

[16] J. Yee and E. Weldon "Evaluation of the performance of error-correcting codes on a Gilbert channel," *IEEE Trans. Commun.,* vol. 43, pp. 2316-2323, Aug. 1995.

[17] W. Turin, *Performance Analysis of Digital Transmission Systems*, New York: Computer Science Press, 1990.

[18] B. D. Fritchman, "A binary channel characterization using partitioned Markov chains," *IEEE Trans. Inform. Theory*, Vol. 13, pp. 221-227, April 1967.

[19] S. Lin and D. Costello Jr., *Error Control Coding: Fundamentals and Applications*, 2nd edition, New Jersey: Prentice-Hall, Inc., 2004.

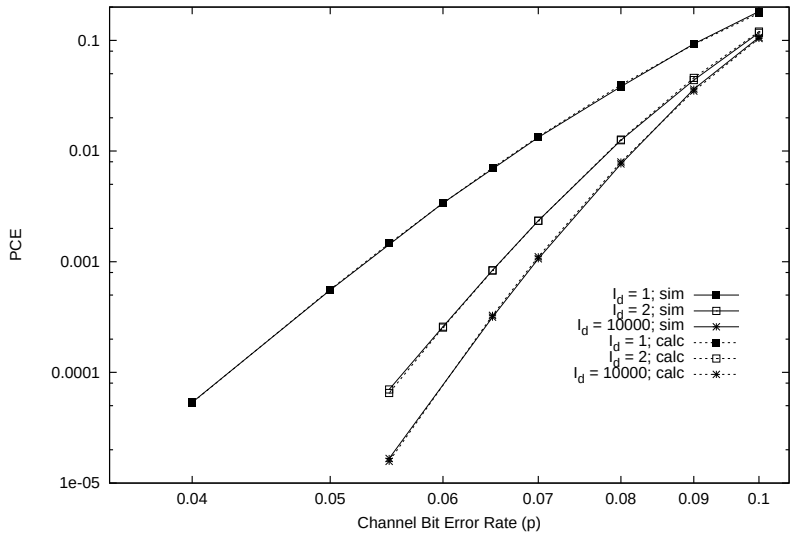

Figure 1: PCE versus p for the symbol interleaved (127,65) RS code with $b = 7$, $t = 31$. Simulation (sim.) and analytical (calc.) results for the BAMNC with $\varepsilon = 0.8$. $I_d = 1, 2, 10000$.

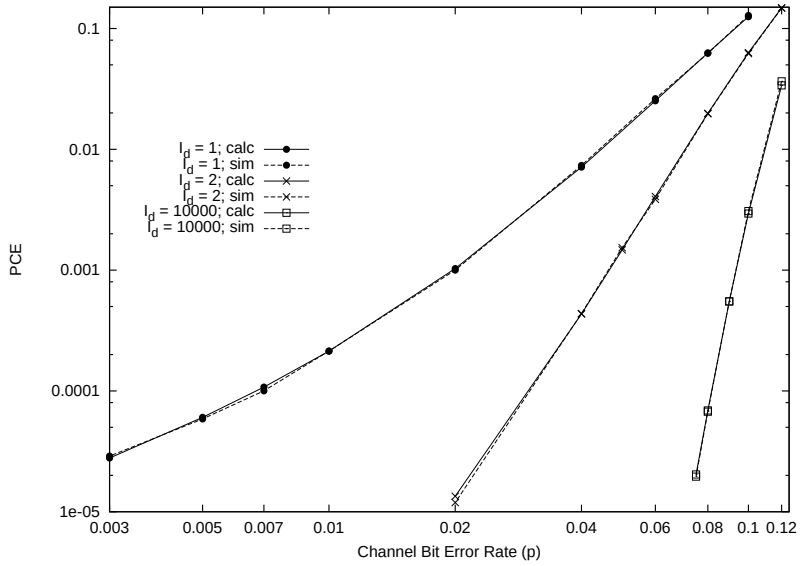

Figure 2: PCE versus p for the symbol interleaved (127,65) RS code with $b = 7$, $t = 31$. Simulation (sim.) and analytical (calc.) results for the QBC with parameters $M = 3$, $\varepsilon = 0.92$, $\alpha = 1$. $I_d = 1, 2, 10000$.

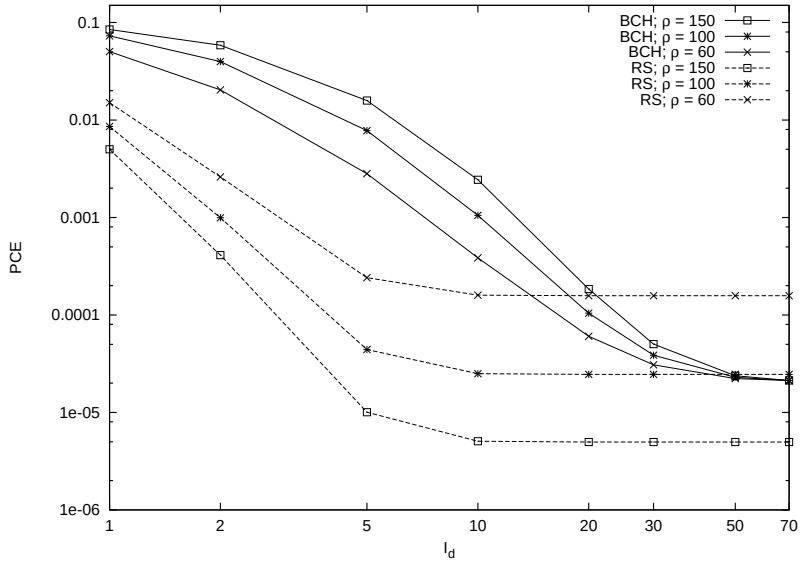

Figure 3: PCE versus I_d for (73,57) RS and (511,394) BCH codes over the GEC with $\mu = 0.9$, BER $= 0.007$, $p_G = 0.001$. $\rho = 60, 100, 150$.

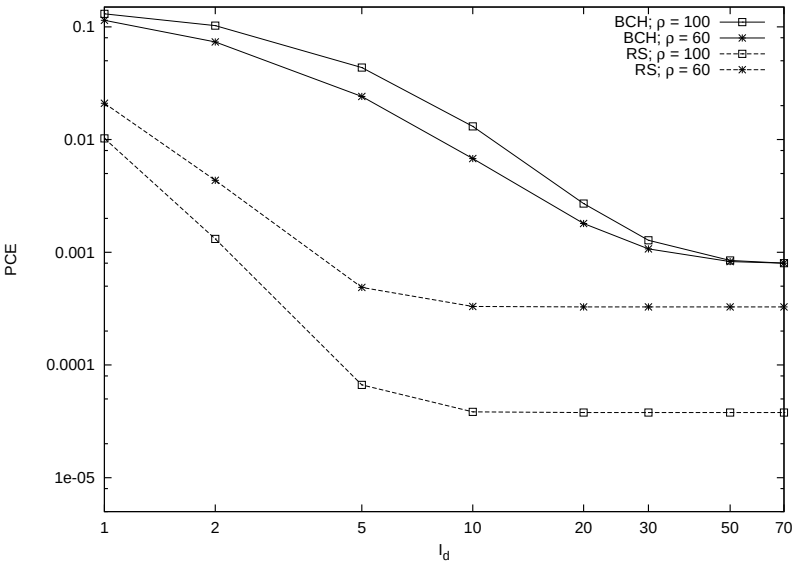

Figure 4: PCE versus I_d for (73,57) RS and (511,394) BCH codes over the GEC with $\mu = 0.9$, BER $= 0.01$, $p_G = 0.001$. $\rho = 60, 100$.

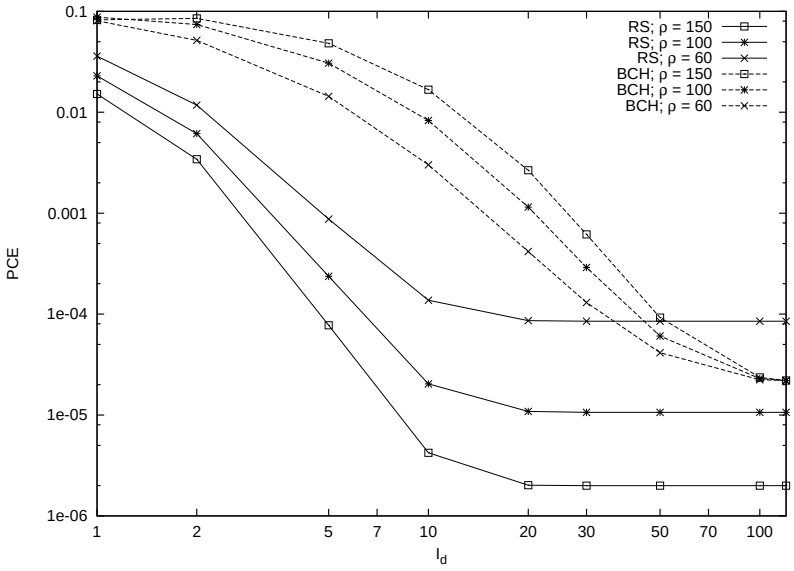

Figure 5: PCE versus I_d for (73,57) RS and (511,394) BCH codes over the GEC with $\mu = 0.95$, BER $= 0.007$, $p_G = 0.001$. $\rho = 60, 100, 150$.

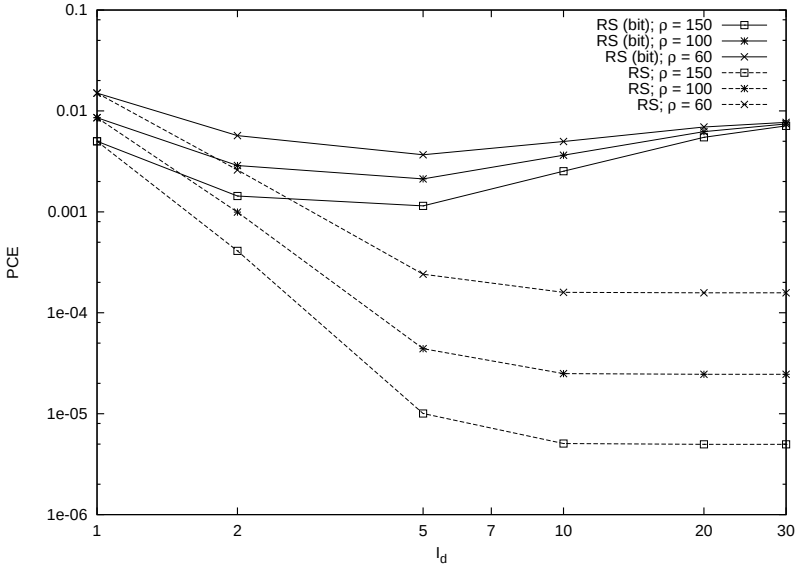

Figure 6: PCE versus I_d for the bit- and symbol-interleaved (73,57) RS code over the GEC with $\mu = 0.9$, BER $= 0.007$, $p_G = 0.001$. $\rho = 60, 100, 150$.