When Can Interleaving Be Avoided for Reed-Solomon Coded Binary Markov Channels ?

Haider Al-Lawati, Fady Alajaji and Cecilio Pimentel
Department of Mathematics and Statistics
Queen's University, Kingston, ON K7L 3N6, Canada
Email: {haider,fady,pimentel}@mast.queensu.ca

***Abstract*— The performance of Reed-Solomon codes over the binary additive Markov noise channel (BAMNC) is analyzed. A recursive expression for the probability of m error symbols in a block of n symbols is derived using the generating series approach, thus facilitating the exact calculation of the probability of codeword error under bounded distance decoding. An approximation to this probability is obtained, and it is shown to be tight when the noise correlation is not very large. In this case, interleaving the channel at the symbol level can be avoided. Furthermore, a wide range of channel conditions, under which channel interleaving at the bit level can be avoided, is identified.**

I. 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]). Conventional communication systems employing these codes are designed for memoryless channels, which is not an accurate model for wireless fading channels. As a consequence, interleaving is used to render the channel memoryless; this introduces additional delay and complexity to the system. Furthermore, such interleaved system fails to exploit the benefits of the statistical memory of the channel noise. 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) and interleaving the code symbols.

The performance of non-interleaved RS codes on correlated fading channels is analyzed in [3]–[6] 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 [3], the channel is modeled via the Gilbert-Elliott channel [7] 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 [4], 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 [5], 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 [6] an L-state Markov chain is proposed to characterize the correlation of symbol errors. Imperfect (finite-length) symbol interleaving is also considered in [4], [5], [8].

The objective of this paper is to identify the range of channel parameters for which perfect interleaving of RS codes (at either the bit or symbol level) does not yield improved performance. To make the analytical derivation simple, we consider the binary additive (first-order) Markov noise channel (BAMNC), but this study can also be conducted for higher-order Markov models which can accurately model correlated fading channels [9]. Using the approach of [5], we first derive a recursive expression for the probability of m error symbols in a block of n symbols and determine the exact PCE when RS codes are sent over the BAMNC. Then we derive an approximation to the PCE under the assumption that the noise within a symbol is Markovian but is independent from symbol to symbol (i.e., the PCE under perfect symbol interleaving). We show that the PCE under perfect symbol interleaving is superior to that under perfect bit interleaving. We compare the approximated PCE with the exact PCE numerically for four different RS codes to find channel conditions – described in terms of the channel bit error rate (CBER) and noise correlation – for which the approximation is accurate. For such conditions, symbol interleaving can be discarded or avoided. Finally, we compare the exact PCE for the BAMNC with the exact PCE for the BSC (the BAMNC under perfect bit interleaving) and determine a wider range of channel parameters under which bit interleaving can be avoided.

II. System Description

A. Channel Model

We consider a BAMNC whose output symbol Y_k at time 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 input symbol and $Z_k \in \{0, 1\}$ is the ith noise symbol. We assume

This work was supported in part by NSERC of Canada and CNPq of Brazil.
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).

that the input and noise processes are independent of each other. Furthermore, we assume that the noise process $\{Z_k\}_{k=1}^{\infty}$ is a stationary (first-order) Markov with transition probability matrix given by

$$\mathbf{P} = [P_{ij}] = \begin{bmatrix} \varepsilon + (1-\varepsilon)(1-p) & (1-\varepsilon)p \\ (1-\varepsilon)(1-p) & \varepsilon + (1-\varepsilon)p \end{bmatrix}$$

where $P_{ij} \triangleq \Pr(Z_k = j | Z_{k-1} = i)$, $i, j \in \{0, 1\}$. Here $p = \Pr(Z_k = 1)$ is the CBER, and $\varepsilon \triangleq [\Pr(Z_k = 1, Z_{k-1} = 1) - p^2]/[p(1-p)]$ is the correlation coefficient of the noise process. We assume that $0 < p < 1/2$ and that $0 \leq \varepsilon < 1$, ensuring that the noise process is irreducible (it is also general in the sense of being equivalent to all stationary binary Markov processes with nonnegative correlation coefficient). When $\varepsilon = 0$, the noise process becomes independent and identically distributed and the resulting channel reduces to the memoryless BSC channel with crossover probability p. The state of the Markov channel at time k is denoted by S_k and given by $S_k = Z_k$. For $z \in \{0, 1\}$, let $\mathbf{P}(z)$ be a 2×2 matrix whose ijth entry is given by $\Pr(Z_k = z, S_k = j | S_{k-1} = i)$. Hence,

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

Note that $\mathbf{P}(0) + \mathbf{P}(1) = \mathbf{P}$. Let $z^n = (z_1, z_2, \cdots, z_n)$ be a binary noise sequence of length n, then

$$\Pr(Z^n = z^n) = \mathbf{\Pi}^T \left(\prod_{i=0}^{n} \mathbf{P}(z_i) \right) \mathbf{1}$$

where the superscript $[\cdot]^T$ indicates the transpose of a matrix, $\mathbf{\Pi} = [1-p, \quad p]^T$ is the stationary distribution, and $\mathbf{1}$ is a column matrix with all entries being 1. This channel model is a special case of the Gilbert-Elliott channel, realized by setting the cross-over probabilities of the "good" and "bad" channel components [7] equal to zero and one, respectively.

B. Reed-Solomon Codes

An (n, k) RS code over the Galois field GF(2^b) is a non-binary linear block code whose codewords are of length $n = 2^b - 1$ symbols. Each codeword contains k information symbols, the rate of the code is $R = k/n$ and the code can correct up to $t = \lfloor \frac{n-k}{2} \rfloor$ symbols (under bounded distance decoding). Each symbol in GF(2^b) can be mapped one-to-one to a binary b-tuple. As a result, the non-binary codewords are sent over the BAMNC by transmitting the equivalent binary representation for each codeword. A transmitted symbol is received correctly if the noise corrupting it is a sequence of zeros of length b. Otherwise, the transmitted symbol is received incorrectly.

III. Performance Analysis

A. Exact Probability of Codeword Error

For a t-error correcting code using bounded distance decoding, the probability of correct decoding P_c and the probability of codeword error 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 $P(s, z) = \sum_{n=0}^{\infty} \sum_{m=0}^{n} P(m, n)\, s^m\, z^n$. For a 2^b-ary code transmitted over a binary finite-state channel, $P(s, z)$ is given by [5]

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

where $\mathbf{I}$ is the 2×2 identity matrix. Thus $P(m, n)$ can be derived as the coefficient of $s^m z^n$ in $P(s, z)$ above [5].

For the BAMNC, it can be shown by induction (see [10]) 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 (1) 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 $\mathbf{I} - z\{\mathbf{P}(0)^b + s(\mathbf{P}^b - \mathbf{P}(0)^b)\}$. Specifically,

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

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

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

If $b = 1$, then we have binary codes, and for this special case $P(m, n)$ reduces to

$$\begin{aligned} &P(m, n) = (\varepsilon + (1-\varepsilon)(1-p)) P(m, n-1) + \\ &(\varepsilon + (1-\varepsilon)p) P(m-1, n-1) - \varepsilon P(m-1, n-2). \end{aligned}$$

This is a simpler expression than the one derived in [10] for the same binary system as it contains one less term.

B. Approximate Probability of Codeword Error

We herein assume that the binary noise process is only Markovian within each symbol (of length b bits), and it is independent between symbols. Obviously, this assumption (which can be realized via perfect symbol interleaving) does not hold when RS codes are directly sent over the BAMNC. Thus, the corresponding $P(m, n)$ for this new system, denoted by $P'(m,n)$, will approximate the actual $P(m,n)$ given in (2). We obtain

$$\begin{aligned} P'(m,n) &= \binom{n}{m} \Pr(1 \text{ symbol error})^m \Pr(\text{No symbol error})^{n-m} \\ &= \binom{n}{m} \left[1-(1-p)[\varepsilon+(1-\varepsilon)(1-p)]^{b-1}\right]^m \\ &\qquad \left[(1-p)[\varepsilon+(1-\varepsilon)(1-p)]^{b-1}\right]^{(n-m)}. \end{aligned} \quad (3)$$

In this case, the probability of correct decoding for a t-error correcting RS code is $P'_c = \sum_{m=0}^{t} P'(m,n)$, while the probability of codeword error for this code (under bounded distance decoding) is simply P$CE' = 1 - P'_c$. Note that when the channel is a BSC (i.e., when $\varepsilon = 0$), this approximation is exact as the channel becomes memoryless.

C. Symbol Interleaving is Always Better than Bit Interleaving

For $0 \le x \le n$, let

$$\begin{aligned} f(x) &\triangleq \left[1-(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}\right]^x \\ &\quad \times \left[(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}\right]^{n-x}, \\ g(x) &\triangleq \left[1-(1-p)^b\right]^x \left[(1-p)^b\right]^{n-x}. \end{aligned}$$

We notice that if $\varepsilon \neq 0$ and $b > 1$, $f(0) > g(0)$ and $f(n) < g(n)$. Also, $g(x)$ is monotone decreasing, constant or monotone increasing with x depending on whether $(1-p)^b$ is larger than, equal to, or less than 1/2, respectively. A similar behavior is observed for $f(x)$ depending on how $(1-p)[\varepsilon + (1-\varepsilon)(1-p)]^{b-1}$ compares with $1/2$. Therefore, if $\varepsilon \neq 0$ and $b > 1$, $(1-p)^b < (1-p)[\varepsilon+(1-\varepsilon)(1-p)]^{b-1}$ and there exists a unique value of x, say x_0, such that $f(x_0) = g(x_0)$. Specifically, x_0 is given by $x_0 = n\,(\ln A / \ln B)$, where

$$A \triangleq \frac{(1-p)^b}{(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}},$$

$$B \triangleq \frac{[1-(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}][1-p]^b}{[(1-p)(\varepsilon+(1-\varepsilon)(1-p))^{b-1}][1-(1-p)^b]}.$$

For example, if $p = 0.01$ and $\varepsilon = 0.3$, then $x_0 = 17.93$ for $b = 8$ and $x_0 = 7.49$ for $b = 7$. Now letting t be an integer less than or equal to $\lfloor x_0 \rfloor$ yields

$$\sum_{i=0}^{t} \binom{n}{i} f(i) > \sum_{i=0}^{t} \binom{n}{i} g(i). \quad (4)$$

The right-hand side of (4) is the probability of correct decoding for a t-error correcting RS code over GF(2^b) when sent over the BSC, while the left-hand side is P'_c. Furthermore, if t is larger than $\lfloor x_0 \rfloor$, then $f(x) < g(x)$ for $t+1 \le x \le n$. Then

$$PCE' = \sum_{i=t+1}^{n} \binom{n}{i} f(i) < \sum_{i=t+1}^{n} \binom{n}{i} g(i) \quad (5)$$

where the right-hand side of (5) is the probability of codeword error for the BSC. Thus we have shown that the code's performance under perfect symbol interleaving is always better when compared with its performance under perfect bit interleaving. This result can also be shown for a larger class of M-order Markov channels [9] as well as the Gilbert-Elliott channel [7].

IV. Results

We consider four RS codes given in Table I. First, we validate our analytical derivation of $P(m,n)$ in (2) by comparing the PCE calculated using $P(m,n)$ with the PCE obtained via simulations (implemented using the Berlekamp-Massey decoding algorithm). The results, shown in Fig. 1 for code C_4 and $\varepsilon = 0.1, 0.9$, indicate a complete agreement between the simulations and the numerical calculations (a similar behavior is observed for the other codes). Thus (2) provides an effective tool for determining PCE without the need for simulations which can be complex and long for low PCE values.

A. When Can Symbol Interleaving Be Avoided ?

Equipped with (2) and (3), we determine the regions of ε and p for which our approximation is accurate (within an absolute relative error less than or equal to 0.1) for the four codes of Table I. In Table II, the (p, ϵ) values for which our approximation is accurate are given in the form $0 \le \epsilon \le \epsilon_{max}$ for values of p chosen so that PCE is between 10^{-5} and 10^{-1}. Thus for these values of (p, ϵ), symbol interleaving can be avoided.

B. When Can Bit Interleaving Be Avoided ?

We evaluate the RS codes of Table I on the BAMNC using (2) to systematically identify the (p, ϵ) values for which the codes performance without interleaving (with $\epsilon > 0$) is superior to that with perfect bit interleaving (with $\epsilon = 0$). The results, with ϵ shown in the form $\epsilon_{min} \le \epsilon \le \epsilon_{max}$ for p given, are summarized in Tables III-VI (the dash symbols in the tables indicate that perfect bit interleaving yields better performance for the specified p value). Thus for such channel conditions, not only can one forgo additional delay and complexity by avoiding bit interleaving, but improved performance can also be achieved as illustrated in Fig. 2.

V. Conclusions

The performance of non-interleaved RS codes over a simple binary channel with memory, the BAMNC, was analyzed and evaluated. It was shown that for any given RS code using standard encoding/decoding procedures (that do not exploit the channel memory), there is a (sometimes wide) range of channel conditions for which the code is well matched to the channel in such way that the code provides the best performance when no (symbol or bit) interleaving is employed. The design of an RS decoding technique that exploits the channel memory can lead to further performance improvements and is an interesting topic for future work.

References

[1] J. Roberts, A. Ryley, D. Jones, and D. Burke, "Analysis of error-correction constraints in an 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] H. Labiod, "Performance of Reed Solomon error-correcting codes on fading channels," *Proc. IEEE Int. Conf. Personal Wireless Commun.*, 1999, pp. 259-263.

[4] 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.

[5] 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.

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

[7] 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.

[8] C. Pimentel and I. F. Blake, “Non-interleaved Reed-Solomon coding performance on finite state channels,” *Proc. IEEE Int. Conf. Commun.*, 1997, pp. 1493-1497.

[9] 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.

[10] 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.

TABLE I

PARAMETERS OF THE CONSIDERED RS CODES.

code	n	k	t	R
C_1	255	221	17	0.867
C_2	255	129	63	0.506
C_3	127	111	8	0.874
C_4	127	65	31	0.511

TABLE II

(p, ε) INTERVALS FOR WHICH TO AVOID SYMBOL INTERLEAVING.

code	p	ε_{max}
C_1	7×10^{-3}	0.2
	5×10^{-3}	0.1
	4×10^{-3}	0.06
C_2	4×10^{-2}	0.3
	3×10^{-2}	0.13
	2.3×10^{-2}	0.06
C_3	1×10^{-2}	0.38
	5×10^{-3}	0.12
	4×10^{-3}	0.08
C_4	4×10^{-2}	0.26
	3×10^{-2}	0.13
	2×10^{-3}	0.04

TABLE III

(p, ϵ) VALUES FOR WHICH TO AVOID BIT INTERLEAVING FOR CODE C_1.

p	ε_{min}	ε_{max}
$\geq 3 \times 10^{-2}$	0	1
3×10^{-3}	0	0.9
2×10^{-3}	0	0.83
1×10^{-3}	0.14	0.62
$\leq 9 \times 10^{-4}$	-	-

TABLE IV

(p, ϵ) VALUES FOR WHICH TO AVOID BIT INTERLEAVING FOR CODE C_2.

p	ε_{min}	ε_{max}
$\geq 5 \times 10^{-2}$	0	1
1×10^{-2}	0	0.87
5×10^{-3}	0	0.73
4×10^{-3}	0	0.64
3.8×10^{-3}	0.11	0.61
3.6×10^{-3}	0.33	0.54
$\leq 3.5 \times 10^{-3}$	-	-

TABLE V

(p, ϵ) VALUES FOR WHICH TO AVOID BIT INTERLEAVING FOR CODE C_3.

p	ε_{min}	ε_{max}
$\geq 5 \times 10^{-3}$	0	1
3×10^{-3}	0	0.87
2×10^{-3}	0	0.78
1.5×10^{-3}	0	0.69
1.2×10^{-3}	0.29	0.53
$\leq 1 \times 10^{-3}$	-	-

TABLE VI

(p, ϵ) VALUES FOR WHICH TO AVOID BIT INTERLEAVING FOR CODE C_4.

p	ε_{min}	ε_{max}
$\geq 5 \times 10^{-2}$	0	1
1×10^{-2}	0	0.82
7×10^{-3}	0	0.73
5×10^{-3}	0.05	0.58
$\leq 4.5 \times 10^{-3}$	-	-

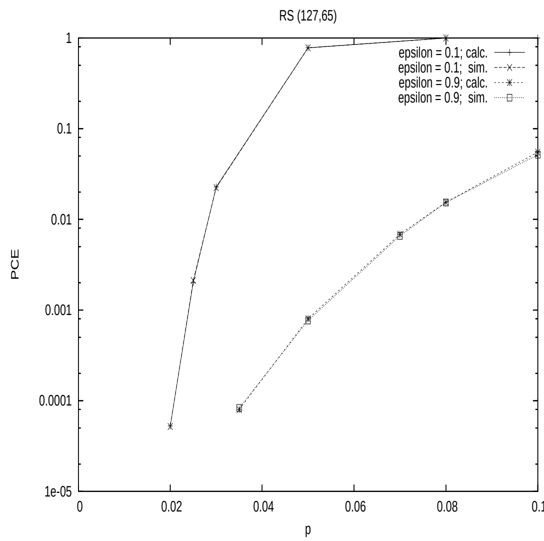

Fig. 1. PCE for code C_4: simulation (sim.) vs analytical (calc.) results.

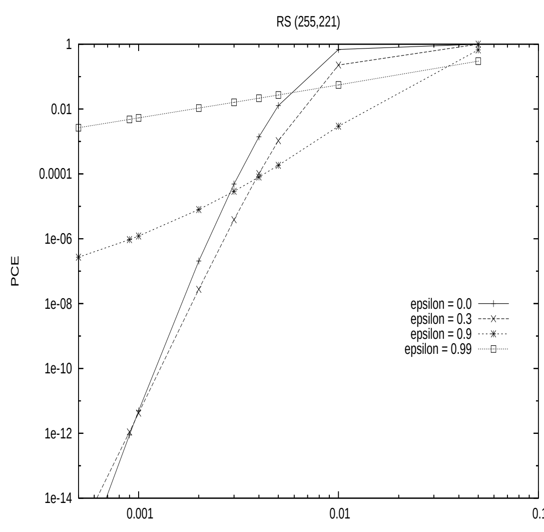

Fig. 2. PCE for code C_1: BAMNC vs BSC.