

GENERATING SERIES FOR ERROR STATISTICS OF BLOCK CODES ON CHANNELS WITH MEMORY

Cecilio Pimentel*

Grupo de Pesquisa em Comunicações - CODEC
Departamento de Eletrônica e Sistemas
Universidade Federal de Pernambuco - UFPE
C. Postal 7800 - Recife - PE - 50711-970
cecilio@npd.ufpe.br

Abstract - We present an analytical method for evaluating the performance of non-interleaved forward error correcting codes on channels that exhibit statistical dependence in the occurrence of errors. We consider a model for such a channel based on the probabilistic function of a Markov chain, also known as finite state channel (FSC) model. The main idea is to apply combinatorial methods to derive simple expressions for the probability of the number of symbol errors produced by the channel in terms of a coefficient in a formal power series. These methods are used to derive expressions for the codeword error probability of various practical coding schemes, including nonbinary block codes and the concatenation of two block codes. The general expressions are specialized for a Gilbert-Elliott channel with known model parameters, and numerical results are derived.

Resumo - Apresentamos um método analítico para calcular o desempenho de códigos corretores de erro em canais que exibem dependência estatística na seqüência de erro. Consideramos um modelo para tais canais baseado em funções probabilísticas de uma Cadeia de Markov, também conhecido como modelo de canais de estados finitos (FSC). A idéia central consiste em aplicar métodos enumerativos para derivar expressões para a probabilidade de erro em termos de coeficientes específicos de uma série de potência formal. Este método é aplicado para calcular o desempenho de vários esquemas de codificação, incluindo códigos não binários e códigos concatenados.

Keywords - Generating series, error correcting codes, Gilbert-Elliott channels, channels with memory, performance of coded systems.

1. INTRODUCTION

The design of reliable communication systems has been an active area of research in the past few years. Among the difficulties encountered by the communication system designer to accomplish this goal, we stress the special system requirements (in general, high carrier frequencies, high data rates, low power consumption are highly desired and sometimes necessary), and the harsh channel environment. For example, in a typical mobile communication scenario, propagation phenomena lead to the presence of signal arriving along dif-

ferent paths, each having random strength, phase and delay. With these system requirements and channel conditions, the combined effect of the channel impairments tend to introduce distortion in the transmitted process in such a way that the errors in the received sequence are grouped together in clusters, called bursts. Because of the statistical dependence in the occurrence of errors, the channel is said to exhibit memory.

To achieve high reliability in data transmission over channels with memory, a good understanding of the channel characteristics is of fundamental importance. The mathematical model for a discrete channel has three constituents: The set of possible discrete inputs to the channel, the set of possible quantized outputs, and the set of probabilities on a sequence of output symbols, conditional on the inputs. The *error sequence* produced by the channel is defined by some measure of difference between the input and output sequence. This error sequence incorporates all the physical impairments and distortions present in the channel.

The discrete channel is the so-called *coded channel*. The discrete inputs and outputs to the coded channel are, respectively, the output sequence of the encoder $\{x_k\}_{k=1}^{\infty}$, and the input sequence to the decoder $\{y_k\}_{k=1}^{\infty}$. Thus, for example, in a binary system the error sequence will be a sequence of zeros and ones defined as follows: At the k -th time interval, the error bit e_k is equal to zero (indicating no error) if $x_k = y_k$, or e_k is equal to one (indicating an error) if $x_k \neq y_k$. The characteristics of the channel impairments, such as a correlated fading process, are incorporated into a mathematical model in such a manner as to produce a statistically similar error sequence as the output of the hard decision receiver.

One important family of discrete mathematical models that has been extensively used to characterize the error sequence is the family of finite state channel (FSC) models [1]. Depending on the application, such models are also referred to as a hidden Markov model, function of Markov chains, and probabilistic automaton. An FSC model is characterized by an underlying non-observable Markov chain. The output symbol of the FSC at the k -th time interval, y_k , is a function of the input symbol x_k and the state of the Markov chain s_k . The channel is described statistically by the conditional probability $P(y_k, s_k | x_k, s_{k-1})$. Each state, s_k , may be associated with a particular channel quality (for example, each state might represent a particular distribution of fading) and the transition of states simulates the time-varying characteristic of the channel.

Several FSC models have been successively used to model

*This work was supported in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 300987/96-0.

practical communication systems, as we can cite: Telephone networks [2], high-frequency microwave links [3, 4], satellite channels [5], magnetic and optical recording systems [6], spread-spectrum frequency-hopped multiple access channels [7], the effect of fading in a mobile radio channel [8, 9, 10], communication systems with loss of synchronization [11], and the burst nature of the Viterbi algorithm decoding [12].

This paper is devoted to the application of the combinatorial methods in the evaluation of the performance of forward error correcting codes over channels modeled as general FSC models. We follow the theory of enumeration of constrained sequences to enumerate a particular subset of error sequences. This powerful and general approach allows us to find a simple formula for the sum of a formal power series, the generating series, where the probabilities of interest are the coefficients of appropriate powers of the indeterminates.

These combinatorial methods are used to derive expressions for the codeword error probability and bounds to symbol and bit error probabilities of various practical coding schemes, including Reed-Solomon (RS) codes and the concatenation of two block codes. Methods for determining the codeword error probability for specific models, as for example, Fritchman [6], and Gilbert-Elliott [2] are known. The contribution of this paper lies in presenting analytical results for the performance of non-interleaved error correcting codes over general FSC models, irrespective the number of states and the structure of the Markov chain. The results of this paper are specialized for a Gilbert-Elliott channel with known model parameters, and numerical results are derived. The substance of this paper comes from work done in a doctoral's thesis [13].

This paper is organized into four sections. A brief review of FSC models and its properties is given in the next section. The performance analysis of coding schemes over FSC models is the main concern of Section 3. Subsection 3.1 is dedicated to analyzing the performance of RS codes. This class of codes are of considerable importance in part because they have an efficient decoding algorithm based on their well-understood algebraic structure. They also have optimum minimum distance since they are maximum distance separable codes. In Subsection 3.2 we investigate the performance of concatenated codes. Finally, Section 4 presents our conclusions to this paper.

2. PROPERTIES OF FINITE STATE CHANNELS

In this section we describe the details of the generation of the error process with FSC models and its properties. The statistical characterization of the error sequence generated by an FSC model will also be discussed.

The input sequence to the channel, denoted as $\{X_k\}_{k=1}^{\infty}$, is transmitted across a binary channel and the corresponding output sequence is $\{Y_k\}_{k=1}^{\infty}$. The impairments due to the channel will be considered as an additive error sequence $\{E_k\}_{k=1}^{\infty}$ and the channel output at the k -th interval is represented as $Y_k = X_k \oplus E_k$. For the cases of interest the alphabet of the symbols X_k , Y_k and E_k is binary, $\mathcal{N}_2 = \{0, 1\}$, and

the symbol \oplus denotes addition modulo 2. An error is said to occur at the k -th time interval whenever $E_k = 1$.

Consider $\{S_k\}_{k=0}^{\infty}$ an N -state, homogeneous, first-order Markov chain with a finite state space $\mathcal{N}_N = \{0, 1, \dots, N-1\}$. This Markov chain is characterized by a set of transition probabilities, $p_{i,j} = P(S_k = j \mid S_{k-1} = i)$, $i, j \in \mathcal{N}_N$, where $p_{i,j}$ is independent upon a particular time interval k . Let \mathbf{P} be an $N \times N$ transition probability matrix, whose (i, j) entry is $p_{i,j}$. We say that a state j can be reached from a state i , if there exists some $n \geq 0$ such that $P(S_{k+n} = j \mid S_k = i) > 0$. A chain is classified as irreducible if, and only if, every state can be reached from every other state [14]. We will now define the period of a state. A state i has period $d(i)$ when $P(S_{k+n} = i \mid S_k = i) = 0$ except when n is multiple of $d(i)$, and $d(i)$ is the largest integer with this property. A chain is aperiodic when all its states have period equal to 1. We consider only irreducible and aperiodic Markov chains. For irreducible and aperiodic Markov chains, there exists a limiting distribution for S_k , as $k \rightarrow \infty$, independent of the starting distribution for S_0 . This limiting distribution is known as the stationary distribution and is denoted by the matrix $\mathbf{\Pi} = [\pi_0 \pi_1 \dots \pi_{N-1}]^T$, where the superscript $[\cdot]^T$ indicates the transpose of a matrix. Additionally, if the initial state S_0 has distribution $\mathbf{\Pi}$, the subsequent states S_k have distribution $\mathbf{\Pi}$ for all k .

Throughout this paper we consider a particular class of FSC models where the error sequence is generated as follows. At the k -th time interval, the chain makes a transition from state $S_{k-1} = s_{k-1}$ to $S_k = s_k$ with probability p_{s_{k-1}, s_k} and generates an output symbol $e_k \in \mathcal{N}_2$ (independent of s_{k-1}), with probability $b_{s_k, e_k} = P(E_k = e_k \mid S_k = s_k)$. The sequence $\{e_k\}_{k=1}^{\infty}$ is known as the observed sequence of the model, and notice that the underlying state sequence cannot be determined from the observed sequence. We assume that the following definitions and properties are valid:

- $$P(E_k = e_k, S_k = s_k \mid S_{k-1} = s_{k-1}, \dots, S_0 = s_0, E_{k-1} = e_{k-1}, \dots, E_1 = e_1) =$$

$$P(E_k = e_k \mid S_k = s_k) P(S_k = s_k \mid S_{k-1} = s_{k-1}) = b_{s_k, e_k} p_{s_{k-1}, s_k}.$$

- The error process is independent of the input sequence (channels that possess this property are called *symmetric channels*). Then

$$\begin{aligned} P(e_k, e_{k+1}, \dots, e_{k+n}) &= \\ &= P(E_k = e_k, E_{k+1} = e_{k+1}, \dots, E_{k+n} = e_{k+n}); \\ &= P(y_k, y_{k+1}, \dots, y_{k+n} \mid x_k, x_{k+1}, \dots, x_{k+n}), \end{aligned}$$

where each error symbol e_k is equal to the difference between the output and input symbols, i.e., $e_k = y_k \oplus x_k$, since in \mathcal{N}_2 \oplus and \ominus are the same.

- The distribution of the initial state is the stationary distribution $\mathbf{\Pi}$. Hence, the error sequence is a stationary process and is completely characterized when the multidimensional probability $P(\mathbf{e}_n) \triangleq P(e_1 e_2 \dots e_n)$ is known for all values of n .

- When conditioned on the state process, the error process is memoryless, that is:

$$P(\mathbf{e}_n | \mathbf{s}_n) = \prod_{k=1}^n P(e_k | s_k).$$

Having established the basic properties of the model, we turn to the problem of calculating the probability of an error sequence. By the law of total probability and the previous definitions, the probability of an error sequence of length n , $\mathbf{e}_n \triangleq e_1 e_2 \dots e_n$, may be expressed as:

$$\begin{aligned} P(\mathbf{e}_n | S_0 = s_0) &= \\ &= \left(\sum_{\mathbf{s}_n \in \mathcal{N}_N^n} P(\mathbf{E}_n = \mathbf{e}_n | \mathbf{S}_n = \mathbf{s}_n, S_0 = s_0) \right. \\ &\quad \left. P(\mathbf{S}_n = \mathbf{s}_n | S_0 = s_0) \right); \\ &= \left(\sum_{\mathbf{s}_n \in \mathcal{N}_N^n} \prod_{k=1}^n P(E_k = e_k | S_k = s_k) \right. \\ &\quad \left. P(S_k = s_k | S_{k-1} = s_{k-1}) \right); \\ &= \sum_{\mathbf{s}_n \in \mathcal{N}_N^n} \prod_{k=1}^n b_{s_k, e_k} p_{s_{k-1}, s_k}. \end{aligned}$$

Hence

$$P(\mathbf{e}_n) = \sum_{s_0=0}^{N-1} \pi_{s_0} \sum_{\mathbf{s}_n \in \mathcal{N}_N^n} \prod_{k=1}^n b_{s_k, e_k} p_{s_{k-1}, s_k}. \quad (1)$$

Equation (1) can also be written using matrix form [11]. Define two $N \times N$ matrices, $\mathbf{P}(0)$ and $\mathbf{P}(1)$, where the (i, j) entry of the matrix $\mathbf{P}(e_k)$ is $P(E_k = e_k, S_k = j | S_{k-1} = i) = b_{j, e_k} p_{i, j}$, which is the probability that the output symbol is e_k when the chain makes a transition from state i to j . Equation (1) has a matrix form given by:

$$P(\mathbf{e}_n) = \mathbf{\Pi}^T \left(\prod_{k=1}^n \mathbf{P}(e_k) \right) \mathbf{1}. \quad (2)$$

The following expressions are valid for the matrices \mathbf{P} and $\mathbf{\Pi}$:

$$\mathbf{P} = \mathbf{P}(0) + \mathbf{P}(1); \quad (3)$$

$$\mathbf{\Pi}^T \mathbf{P} = \mathbf{\Pi}^T; \quad (4)$$

$$\mathbf{P} \mathbf{1} = \mathbf{1}; \quad (5)$$

$$\mathbf{\Pi}^T \mathbf{1} = 1. \quad (6)$$

>From (4) and (5) we conclude that the vectors $\mathbf{\Pi}^T$ and $\mathbf{1}$ are the left and right eigenvectors of the matrix \mathbf{P} , respectively, corresponding to the eigenvalue 1. A binary stationary FSC model is completely specified by the matrices $\mathbf{P}(0)$ and $\mathbf{P}(1)$, since the initial distribution is the unique solution of Equation (4), and \mathbf{P} is given by Equation (3).

Various burst channel models have been proposed in the past few decades. The first model, based on a binary probabilistic function of a Markov chain, was proposed in 1960 by Gilbert [15] in his studies to characterize the telephone channel. The Gilbert channel model, or, for short, the Gilbert channel, is a two-state Markov chain composed of an error-free (good) and an error (bad) state. When the chain is in the good state the error bit e_k is always zero. Otherwise, when it is in a bad state, the error bit is zero (no error) with probability $1 - b$, or one (error) with probability b . The Gilbert

channel was generalized by Elliott [2] in 1963, yielding the well known Gilbert-Elliott channel, by introducing a parameter g , which is the probability that the error bit is one (error) when the chain is in a good state. A further generalization was proposed by McCullough [16], whose model differs from Gilbert-Elliott's channel essentially in two ways: (i) more than one bad state is considered, (ii) transition between states are permitted only immediately after an error. In spite of its simplicity, the derivation of expressions for certain error statistics can be surprising difficult and closed form expressions for quantities such as capacity, are not known at all.

A comprehensive presentation of many mathematical models proposed in the sixties and seventies is given in [1]. In the following example we specialize the equations developed in this section for the Gilbert-Elliott channel.

2.1. EXAMPLE: THE GILBERT-ELLIOTT CHANNEL

The Gilbert-Elliott channel [2, 15] consists of a two-state Markov chain. The state space is $\mathcal{N}_2 = \{0, 1\}$, and $b_{0,1} = g$, and $b_{1,1} = b$, as shown in Figure 1. The model has four parameters Q, g, b, g . By definition, $g < b$ (the state 0 is the good state).

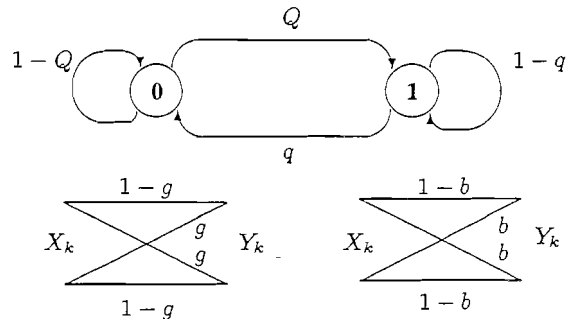


Figure 1. Gilbert-Elliott model for burst channels.

The matrices \mathbf{P} , $\mathbf{P}(0)$, $\mathbf{P}(1)$ and $\mathbf{\Pi}$ are given by:

$$\mathbf{P} = \begin{bmatrix} 1-Q & Q \\ q & 1-q \end{bmatrix}; \quad (7)$$

$$\mathbf{P}(0) = \begin{bmatrix} (1-Q)(1-g) & Q(1-b) \\ q(1-g) & (1-q)(1-b) \end{bmatrix}; \quad (8)$$

$$\mathbf{P}(1) = \begin{bmatrix} (1-Q)g & Qb \\ qg & (1-q)b \end{bmatrix}; \quad (9)$$

$$\mathbf{\Pi} = \begin{bmatrix} \pi_0 \\ \pi_1 \end{bmatrix} = \begin{bmatrix} \frac{q}{q+Q} \\ \frac{Q}{q+Q} \end{bmatrix}. \quad (10)$$

Some error distributions for this channel can be calculated using Equation (2). As an example, the probability the bit error is a 1, $P(1) \triangleq P(E_k = 1)$, and the probability of two consecutive ones, $P(11) \triangleq P(E_k = 1, E_{k+1} = 1)$, are given

by:

$$P(1) = \mathbf{\Pi}^T \mathbf{P}(1) \mathbf{1} = \pi_0 g + \pi_1 b; \quad (11)$$

$$= \frac{1}{1+\frac{1}{\rho}} g + \frac{1}{1+\rho} b.$$

$$P(11) = \mathbf{\Pi}^T \mathbf{P}(1) \mathbf{P}(1) \mathbf{1} = \pi_0 g[(1-Q)g + Qb] + \pi_1 b[qg + (1-q)b].$$

In Equation (11) ρ is the good-to-bad ratio defined as:

$$\rho \triangleq P(S_k = 0)/P(S_k = 1) = \pi_0/\pi_1 = q/Q. \quad (12)$$

The performance evaluation of a coded communication system operating over an FSC model will be discussed in the next section. We will derive expressions for the probability of codeword error through the determination of $P_s(m, n)$, the probability of m channel error symbols in a block of length n symbols. A general model is described by a set of matrices $\mathbf{\Pi}$, $\mathbf{P}(0)$, $\mathbf{P}(1)$ and the probability $P_s(m, n)$ is expressed as a coefficient of particular terms in a formal power series.

3. PERFORMANCE ANALYSIS

We now establish some notation. $\mathbf{0}_n$ denotes the sequence of 0's of length n , for example, $\mathbf{0}_2 = 00$. Let R be the field of real numbers. If s and z are commutative indeterminates, $[s^k z^n] P(s, z)$ denotes the coefficient of $s^k z^n$ in the formal power series $P(s, z)$. Let $R \langle x_0, x_1 \rangle$ be the set of polynomials in non-commuting indeterminates x_0 and x_1 , that is, the set of all sums of finite non-commuting products of x_0 and x_1 with coefficients taken from R . It is easy to see that $R \langle x_0, x_1 \rangle$ together with the operations of addition and multiplication is a ring. For convenience, this ring is denoted by $R \langle x_0, x_1 \rangle$. If \mathcal{E}_n is a set of binary sequences of length n , denote the generating series for \mathcal{E}_n by:

$$F_{\mathcal{E}_n} = \sum_{\mathbf{e}_n \in \mathcal{E}_n} x_{e_1} x_{e_2} \cdots x_{e_n} \in R \langle x_0, x_1 \rangle, \quad (13)$$

where $x_{e_i} \in \{x_0, x_1\}$ and the indeterminates x_0 and x_1 mark an error bit produced by the channel. For example, if \mathcal{E}_4 is the subset of \mathcal{N}_2^4 defined as $\mathcal{E}_4 = \{\text{one error in a block of length 4}\}$, then $\mathcal{E}_4 = \{1000, 0100, 0010, 0001\}$. According to the definition of $F_{\mathcal{E}_n}$ in (13) the generating series for the set \mathcal{E}_4 is:

$$F_{\mathcal{E}_4} = \{x_1 x_0^3 + x_0 x_1 x_0^2 + x_0^2 x_1 x_0 + x_0^3 x_1\}.$$

Consider that the error sequence is generated by an N -state binary FSC model defined in terms of the matrices $\mathbf{\Pi}$, $\mathbf{P}(0)$, $\mathbf{P}(1)$. From Equations (2) the probability of the set \mathcal{E}_4 defined above may be expressed as:

$$P(\mathcal{E}_4) = \mathbf{\Pi}^T \{ \mathbf{P}(1) \mathbf{P}(0)^3 + \mathbf{P}(0) \mathbf{P}(1) \mathbf{P}(0)^2 + \mathbf{P}(0)^2 \mathbf{P}(1) \mathbf{P}(0) + \mathbf{P}(0)^3 \mathbf{P}(1) \} \mathbf{1}.$$

Notice that $P(\mathcal{E}_n)$ may be obtained from the generating series $F_{\mathcal{E}_n}$ simply by replacing x_{e_i} by $\mathbf{P}(e_i)$ and wrapping the

vector $\mathbf{\Pi}^T$ around the front and $\mathbf{1}$ around the back. We can formalize this concept by defining the mapping:

$$\Delta : R \langle x_0, x_1 \rangle \longrightarrow M_N(R) : x_k \mapsto \mathbf{P}(k), \quad (14)$$

acting as a homomorphism to the whole of the ring $R \langle x_0, x_1 \rangle$. $M_N(R)$ is the ring of all $N \times N$ matrices with entries taken from R . The probability of the set \mathcal{E}_n may be expressed very compactly as:

$$P(\mathcal{E}_n) = \mathbf{\Pi}^T (\Delta F_{\mathcal{E}_n}) \mathbf{1}. \quad (15)$$

An expression for $P(\mathcal{E}_n)$ can be written down directly from the generating series $F_{\mathcal{E}_n}$ in non-commuting indeterminates by acting on $F_{\mathcal{E}_n}$ with the homomorphism Δ , and then wrapping $\mathbf{\Pi}^T$ and $\mathbf{1}$ around it. Therefore, the main step to find $P(\mathcal{E}_n)$ is to determine the generating series $F_{\mathcal{E}_n}$.

We now develop an expression for $P_s(m, n)$ for two cases: RS codes and concatenated codes.

3.1. NONBINARY CODES

An (n, k) nonbinary code defined over the Galois field $\text{GF}(2^c)$, where c is a positive integer, has codewords of length n symbols, k information symbols, $n - k$ parity check symbols, and code rate $R_c = k/n$. For example, an primitive RS code has length $n = 2^c - 1$ symbols and can correct any combination of up to $t = \lfloor (n - k)/2 \rfloor$ error symbols within a codeword, where t denotes the error correcting capability of the code, and $\lfloor x \rfloor$ is the greatest integer less than or equal to x .

We consider a coded communication system where nonbinary transmitted symbols, taking values on $\text{GF}(2^c)$, are transmitted across a binary channel. Each symbol in a transmitted codeword is corrupted by an additive error symbol e_k , composed of a sequence of c error bits statistically distributed according to the FSC model. Each error symbol e_k can also be regarded as an element from $\text{GF}(2^c)$, where each sequence of c bits is the vector-space representation of the corresponding field element. The k -th received symbol within a codeword is the sum $z_k = c_k + e_k$, $z_k \in \text{GF}(2^c)$, where the addition is over $\text{GF}(2^c)$. The transmitted symbol is received correctly (i.e., $z_k = c_k$) if the symbol e_k is the sequence of c consecutive zeros, denoted by $\mathbf{0}_c$. Otherwise, if $e_k \neq \mathbf{0}_c$ the transmitted symbol is received incorrectly. Due to this symbol orientation, RS codes are suited to an environment where both burst and random errors occur. An expression for the probability of m erroneous received symbols in a block of length n , $P_s(m, n)$, is developed next.

Let F_c and F_e denote the generating series for sets of error symbols e_k that produce a correct and an erroneous received symbol, respectively. Then

$$\begin{aligned} F_c &= x_0^c \in R \langle x_0, x_1 \rangle; \\ F_e &= (x_0 + x_1)^c - x_0^c \in R \langle x_0, x_1 \rangle, \end{aligned} \quad (16)$$

where the indeterminates x_0 and x_1 mark an error bit (produced by the channel) equal to 0 or 1, respectively. The set of all error symbol patterns of any length is $(1 - F_c - F_e)^{-1}$. Notice that $P_s(m, n)$ is equal to the probability that m error symbols from the set enumerated by F_e occur in a block of

n consecutive error symbols. Let the indeterminate z mark the length of an error word (an n -tuple of error symbols over $GF(2^c)$), and let s mark the number of error symbols from the set enumerated by F_e in an error word. Then, from the mapping Δ defined in Equation (14), and from Equation (15), $P_s(m, n)$ may be expressed as:

$$P_s(m, n) = [s^m z^n] \Pi^T \Delta (1 - z(F_c + sF_e))^{-1} \mathbf{1} \quad (17)$$

$$= [s^m z^n] \Pi^T \Delta (1 - z \{x_0^c + s((x_0 + x_1)^c - x_0^c)\})^{-1} \mathbf{1} \quad (18)$$

$$= [s^m z^n] \Pi^T (\mathbf{I} - z \{P(0)^c + s(P^c - P(0)^c)\})^{-1} \mathbf{1}. \quad (19)$$

From Equation (19) it is simple to derive recurrence formulas for $P_s(m, n)$, which provides a rapid computational scheme for the problem. For a specific FSC model, $P_s(m, n)$ can be expressed as $[s^m z^n] P(s, z)$, where $P(s, z)$ is the ratio of two polynomials in s and z . The denominator polynomial is responsible for the recurrence relation, and the numerator polynomial defines the initial conditions. For example, it is easy to show that $P_s(m, n)$ for a two-state Gilbert-Elliott channel satisfies a six-term recurrence formula. For example, the recurrence formula for $c = 1$ (binary code) is given by:

$$\begin{aligned} P(m, n) = & \\ & -(Q(1-g) + q(1-b) - (2-g-b))P(m, n-1) \\ & + (b(1-q) + g(1-Q))P(m-1, n-1) \\ & - ((1-b)(1-g)(1-q-Q))P(m, n-2) \\ & - ((1-q-Q)(b+g-2gb))P(m-1, n-2) \\ & - ((1-q-Q)gb)P(m-2, n-2), \end{aligned}$$

Figure 2. shows $P_s(m, n)$, as a function of m , for Gilbert-Elliott channels with various values of memory, $\mu = (1 - q - Q)$, for $n = 127$, and $c = 7$. Throughout this section we consider the following model parameters, $\rho = q/Q = 20$, $b = 0.4$, $g = 0.001$. The parameters Q and q are uniquely determined from μ and ρ . Because the Gilbert-Elliott channel has a parameter that can be interpreted as the memory of the channel, the effectiveness of coding schemes under several memory conditions can be evaluated.

The average number of erroneous symbols in a received word of length n is $\bar{n}_s = n \Pi^T (P^c - P(0)^c) \mathbf{1}$. Examples of values of \bar{n}_s are 12 for $\mu = 0.6$, 10 for $\mu = 0.8$, 8 for $\mu = 0.92$, 7 for $\mu = 0.96$. The curves of Figure 2. show that for values of μ approximately less than 0.8 the probability $P_s(m, 127)$ has a maximum roughly centered around \bar{n}_s . This is a typical behavior of memoryless channels. Therefore, over the span of $127 \times 7 = 889$ bits, models with $\mu < 0.8$ make sufficient state transitions to assure this "random" behavior. However, when the memory increases, fewer transitions occur between states and long bursts are more likely. As a consequence, $P_s(m, 127)$ spreads out and decreases slowly with m . To give an example, the curves show that $P_s(0, 127) = 0.36$ for $\mu = 0.99$. This is the probability of being in the good state during all 889 bit intervals and making no error, which is equal to, $\pi_0((1-Q)(1-g))^{889} = 0.36$. The contribution of any other state sequence to $P_s(m, 127)$ is negligible. In the sequel we discuss how the amount of memory affects the codeword error probability of RS codes.

We consider the case of bounded-distance decoding: Given a received word, the decoder selects a codeword which lies within Hamming distance t of the received word. If no such

codeword exists a *decoding failure* is declared. The decoder decodes the received word as the correct (transmitted) codeword if no more than t error symbols occur in one codeword. The probability of codeword error (PCE) is defined as the probability of occurrence of received words with more than t erroneous symbols. Thus

$$PCE = 1 - \sum_{m=0}^t P_s(m, n) = \sum_{m=t+1}^n P_s(m, n). \quad (20)$$

Figure 3.2. shows PCE for RS codes with fixed length n , versus the memory μ , for various values of k (number of information symbols). In this analysis we consider $PCE = 10^{-6}$ the required error probability for reliable communication. We can conclude from these plots that for a particular value of μ , say $\mu = 0.92$, PCE equals to 10^{-6} is achieved with rate $R_c = 49/127 = 0.39$ for $c = 7$ ($n = 127$), and $R_c = 141/255 = 0.55$ for $c = 8$ ($n = 255$).

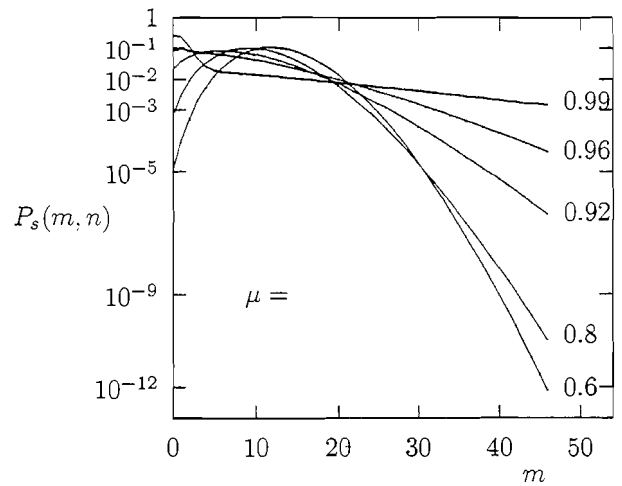


Figure 2. $P_s(m, n)$ as a function of m , for $n = 127$, having the memory μ as a parameter, $\mu = 0.6, 0.8, 0.92, 0.96, 0.99$.

It was also observed that for a fixed k , PCE is minimum for $\mu = 0.6$. In fact, the curves show two distinct modes of behavior of PCE, depending upon the burst length. In the region of short bursts, say $\mu < 0.6$, as the memory increases the error bits become more concentrated within bursts and affect fewer symbols in a codeword. Therefore, short bursts help the performance of RS decoders. On the other hand, in the region of high memory, say $\mu > 0.8$, where long bursts occur, reliable communication is possible only with longer low rate codes.

In this section we have used PCE as a measure of performance. The evaluation of other important measures will be discussed in the next subsection.

3.2. AN UPPER BOUND TO THE SYMBOL AND BIT ERROR PROBABILITIES

Error control strategies are typically compared on the basis of various probabilistic measures of performance. In addition to PCE, the symbol error probability P_s , and the bit error probability P_b , are also important measures in evaluating system

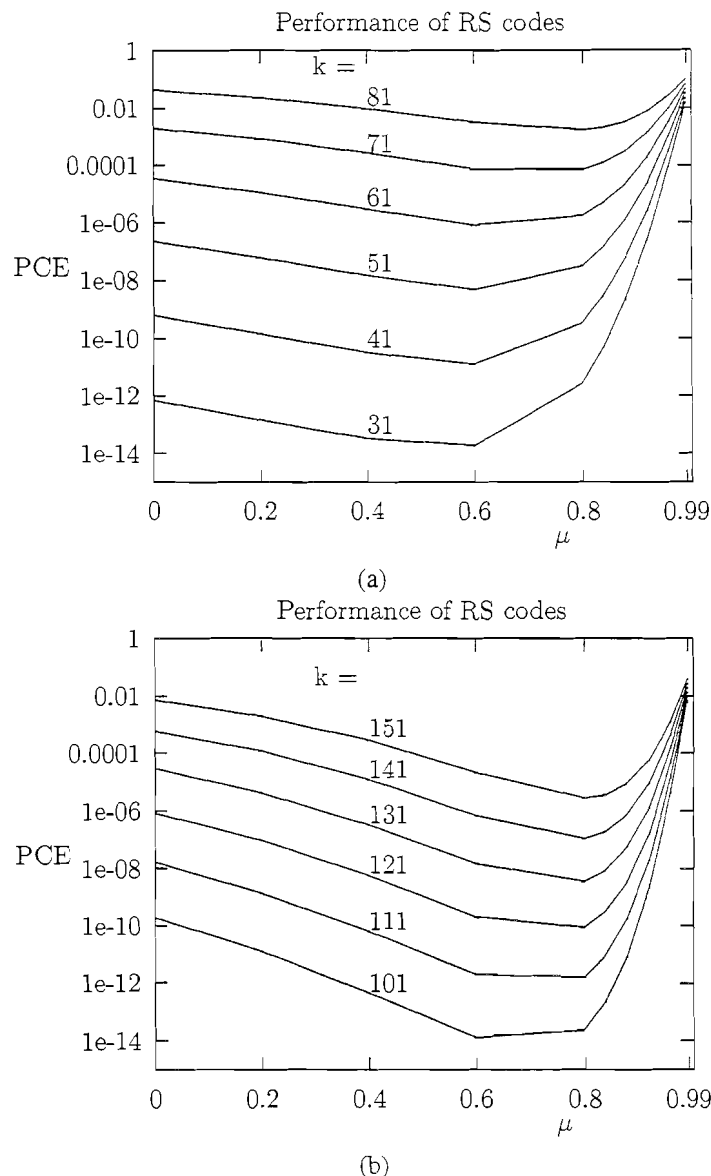


Figure 3. PCE versus memory μ , for RS codes over Gilbert-Elliott channels having the number of information symbols k as a parameter, for $c = 7$ (a); $c = 8$ (b).

performance [17]. An exact expression for either P_s or P_b is in general difficult to evaluate, since it depends to a large extent on the operation of the decoding algorithm. Expressions for P_b are available in the literature for block codes on memoryless channels with known codeword weight distribution [18]. In this section, a simple upper bound on P_b and P_s that does not depend upon the decoding operation is presented.

Let $\mathbf{c} = (c_1, \dots, c_n)$, $\mathbf{z} = (z_1, \dots, z_n)$, and $\hat{\mathbf{c}} = (\hat{c}_1, \dots, \hat{c}_n)$ be the transmitted codeword, the received word, and the codeword chosen by the decoder, respectively. The average decoded-symbol error probability is defined by [19]:

$$P_s = \frac{1}{n} \sum_{j=1}^n P(c_j \neq \hat{c}_j) = \frac{\mathbf{E}\{N_c\}}{n}, \quad (21)$$

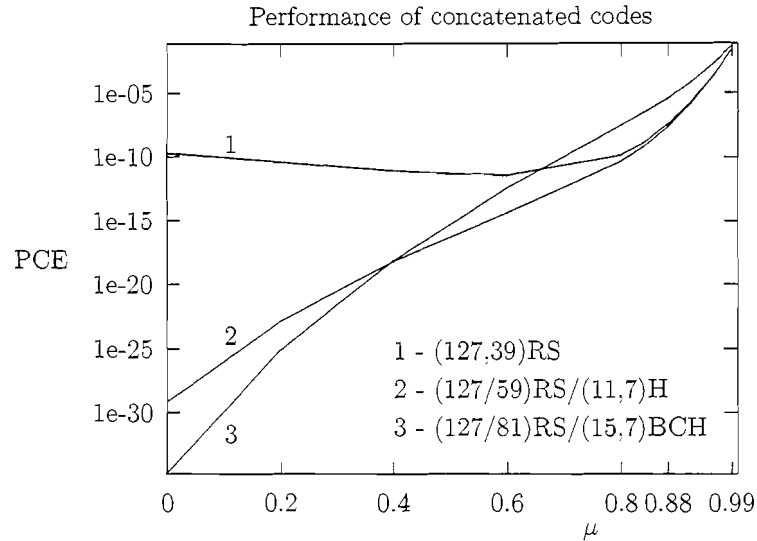
where the random variable N_c is the number of symbols where \mathbf{c} and $\hat{\mathbf{c}}$ differ, and $\mathbf{E}\{\cdot\}$ stands for the expected value

of a random variable. If the random variable N_e is the number of symbol errors in the received word, then

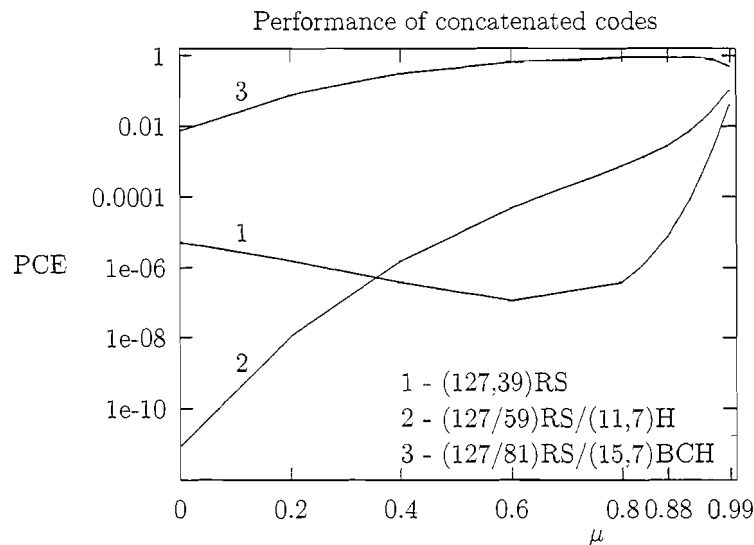
$$P_s = \frac{\mathbf{E}\{\mathbf{E}\{N_c | N_e\}\}}{n} \quad (22)$$

$$= \frac{1}{n} \sum_{m=t+1}^n \mathbf{E}\{N_c | N_e = m\} P_s(m, n). \quad (23)$$

For the case of a t -error correcting bounded-distance decoding, a simple upper bound to $\mathbf{E}\{N_c | N_e = m\}$ is given by the following worst-case argument: Whenever t or more errors occur, the received word lies within a sphere of a wrong (not transmitted) codeword, and that the decoder introduces t additional errors. Clearly, the maximum value assumed by



(a)



(b)

Figure 4. PCE as a function of memory for non-interleaved concatenated codes over the Gilbert-Elliott channel. $R_c = 0.3$ (a); $R_c = 0.45$ (b).

symbol c_i is treated as a binary sequence of length K and is encoded into a codeword of an (N, K) inner code over $GF(2)$. The resulting code has length nN bits and the overall code rate of the concatenated code is $R_c = (K/N)(k/n)$. The decoding method is also done in two steps. The received binary sequence of nN bits at the input to the inner decoder is partitioned into n binary strings of length N (received words of the inner decoder). The operation of the inner decoder can be seen as a memoryless mapping from this string of length N to a symbol z_i in $GF(2^K)$, the RS received symbol. A sequence of n consecutive symbols z_i forms the outer received word and is decoded by the RS decoder.

To evaluate the performance of non-interleaved concatenated codes recall that the probability $P_s(m, n)$ of m erroneous received symbols at the input to the RS decoder is

given by Equation (17). The generating series F_c and F_e for the sets of error symbols that produces a correct and erroneous received RS symbol for the outer channel are:

$$\begin{aligned}
 F_c &= \sum_{0 \leq i \leq T_i} [w^i] (x_0 + wx_1)^N, & \in R < x_0, x_1 >; \\
 F_e &= (x_0 + x_1)^N - F_c, & \in R < x_0, x_1 >.
 \end{aligned}
 \tag{26}$$

In Equation (26), T_i is the error correcting capability of the inner code and the indeterminate w marks the number of error bits in a received word of length N at the input to the inner decoder. Notice that F_c enumerates the correctable error patterns of the inner decoder, that is, all error patterns of length

N and weight less than or equal to T_i . Formulas (26) and (17) have been used to calculate PCE of concatenated codes.

Figure 3.3. depicts the performance of concatenated codes with the same overall code rate. The code rates selected are $R_c = 0.3$ and $R_c = 0.45$. The outer code is the $(127, k)$ RS code, $c = 7$. The inner codes selected are the $(11, 7)$ shortened Hamming code ($T_i = 1$), and the $(15, 7)$ BCH code ($T_i = 2$). As a comparison, the performance of RS codes alone with the same rate is also shown. Notice that the concatenated code uses RS codes with higher rates than the RS code alone, therefore, its decoding complexity is considerably lower. We conclude from Figure 3.3. that, when $R_c = 0.3$, the concatenated code with the Hamming inner code gives the best performance for $\mu > 0.4$. On the other hand, when $R_c = 0.45$, the RS code alone performs better for $\mu > 0.36$. We attribute this to the fact that when the overall code rate increases, the improvements caused by the inner code do not make up the reduction in the number of redundant symbols of the outer RS code.

4. CONCLUSIONS

We have addressed the problem of evaluating the codeword error probability of error control schemes on general FSC models. The main idea to find an expression for this measure for a specific coding scheme is to express the probability of the correctable error pattern as a coefficient in a formal power series. All numerical plots presented in this paper were generated by first deriving recurrence formulas from matrix expressions. Bounds on symbol and bit error probabilities can also be derived using the expressions given in Subsection 3.2..

In the first part of Section 3 we have derived an expression for the codeword error probability of non-interleaved RS codes. The results presented in this section have been applied to investigate the code error-correcting capability necessary to achieve a desired performance. These results were extended to the case of concatenated codes with binary block codes as the inner code. The comparisons reported in this paper among different coding schemes are only valid for the specific channel parameters considered. Clearly, the analysis can be repeated for any FSC model of interest, and other coding schemes can be treated as well with the machinery we have presented in this work.

Acknowledgment

The author would like to express his appreciation to the anonymous reviewers for their helpful comments on an early draft of this paper.

REFERENCES

- [1] L. N. Kanal and A. Sastry, "Models for channels with memory and their applications to error control," *Proceedings of the IEEE*, vol. 66, pp. 724–744, July 1978.
- [2] E. O. Elliott, "Estimates of error rates for codes on burst-noise channels," *The Bell System Technical Journal*, vol. 42, pp. 1977–1997, September 1963.
- [3] B. D. Fritchman, "A binary channel characterization using partitioned Markov chains," *IEEE Transactions on Information Theory*, vol. 13, pp. 221–227, April 1967.
- [4] S. Tsai, "Markov characterization of the HF channel," *IEEE Transactions on Communication Technology*, vol. 17, pp. 24–32, February 1969.
- [5] A. R. K. Sastry, "Performance of hybrid error control schemes on satellite channels," *IEEE Transactions on Communications*, vol. 23, pp. 689–694, July 1975.
- [6] A. I. Drukarev and K. P. Yiu, "Performance of error-correcting codes on channels with memory," *IEEE Transactions on Communications*, vol. 34, pp. 513–521, June 1986.
- [7] M. V. Hegde and W. E. Stark, "Capacity of frequency-hop spread-spectrum multiple-access communication systems," *IEEE Transactions on Communications*, vol. 38, pp. 1050–1059, July 1990.
- [8] J.-Y. Chouinard, M. LeCours, and G. Y. Delisle, "Estimation of Gilbert's and Fritchman's models parameters using the gradient method for digital mobile radio channels," *IEEE Transactions on Vehicular Technology*, vol. 37, pp. 158–166, August 1988.
- [9] F. Swarts and H. C. Ferreira, "Markov characterization of channels with soft decision outputs," *IEEE Transactions on Communications*, vol. 41, pp. 678–681, May 1993.
- [10] F. Swarts and H. C. Ferreira, "Markov characterization of digital fading mobile VHF channels," *IEEE Transactions on Vehicular Technology*, vol. 43, pp. 977–985, November 1994.
- [11] W. Turin and R. M. M. Sondhi, "Modeling error sources in digital channels," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 340–347, April 1993.
- [12] C. Chao and Y. Yao, "Hidden Markov models for the burst error statistics of Viterbi decoding," in: *ICC*. (Geneva, Switzerland), pp. 751–755, May 1993.
- [13] C. Pimentel, "Enumeration Techniques for Finite State Channels". PhD thesis, University of Waterloo, July 1996.
- [14] W. Feller, *An Introduction to Probability Theory and its Applications*. New York: John Wiley and Sons, third ed., 1968.
- [15] E. N. Gilbert, "Capacity of a burst-noise channel," *The Bell System Technical Journal*, vol. 39, pp. 1253–1265, September 1960.
- [16] R. W. McCullough, "The binary regenerative channel," *The Bell System Technical Journal*, vol. 47, pp. 1713–1735, October 1968.

- [17] E. R. Berlekamp, "The technology of error-correcting codes," *Proceedings of the IEEE*, vol. 68, pp. 564–593, May 1980.
- [18] E. Lutz, "Code and interleaver design for data transmission over fading channels," in *Proceedings of the IEEE Global Telecommunications Conference - GLOBECOM*, (Atlanta - GA), pp. 12.4.1–12.4.6, November 1984.
- [19] D. J. Torrieri, "The information-bit error rate for block codes," *IEEE Transactions on Communications*, vol. COM-32, pp. 474–476, April 1984.
- [20] G. D. Forney, Jr., *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.
- [21] C. D. Frank and M. B. Pursley, "Concatenated coding for frequency-hop spread-spectrum with partial band interference," *IEEE Transactions on Communications*, vol. 44, pp. 377–387, March 1996.
- [22] S. Solimar and K. Mokrani, "Performance of coded systems over fading dispersive channels," *IEEE Transactions on Communications*, vol. 40, pp. 51–59, January 1992.
- [23] G. W. Zeoli, "Coupled decoding of block-convolutional concatenated codes," *IEEE Transactions on Communications*, vol. COM-21, pp. 219–226, March 1973.
- [24] M. Herro, D. Costello, Jr, and L. Hu, "Capacity and cutoff rate calculations for a concatenated coding schemes," *IEEE Transactions on Information Theory*, vol. 34, pp. 212–222, March 1988.

Cecilio Pimentel was born in Recife, Brazil, on June 7, 1966. He received the B.Sc degree from the Federal University of Pernambuco, Brazil, in 1987, the M.Sc degree from the Catholics University of Rio de Janeiro, Brazil, in 1990 and the Ph.D. degree from the University of Waterloo, Ontario, Canada, in 1996, all in electrical engineering. Since October 1996, he has been with the Department of Electronics and Systems at the Federal University of Pernambuco. His research interests include digital communications, information theory, and error correcting coding.