International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:6, No:8, 2012

Performance of Block Codes Using the Eigenstructure of the Code Correlation Matrix and Soft-Decision Decoding of BPSK

Vitalice K. Oduol, and Cemal Ardil

Abstract**—**A method is presented for obtaining the error probability for block codes. The method is based on the eigenvalue-eigenvector properties of the code correlation matrix. It is found that under a unary transformation and for an additive white Gaussian noise environment, the performance evaluation of a block code becomes a one-dimensional problem in which only one eigenvalue and its corresponding eigenvector are needed in the computation. The obtained error rate results show remarkable agreement between simulations and analysis.

Keywords**—**bit error rate, block codes, code correlation matrix, eigenstructure, soft-decision decoding, weight vector.

I. Introduction

THE topic of error control codes, both block and convolutional codes is a mature subject on which there have been many papers and books [1-6]. The computation of the post-decoding bit error rate (BER) is usually accomplished using performance bounds. Although many of these bounds can be very tight, it is still better when an exact result can be found.

The method presented here obtains the exact probability of error for block codes using soft-decision decoding in an additive white Gaussian noise environment. It is based on the eigen-structure of the code correlation matrix, in that the eigenvalue-eigenvector properties determine the relevant parameters needed in the performance evaluation. It is found that under a suitable unitary transformation of the decision variables the performance evaluation of a block code becomes a one-dimensional problem in which only the dominant eigenvalue and its corresponding eigenvector are needed.Only the dimension corresponding to the largest eigenvalue need be considered, all others having collapsed to a point. Use is made of the fact that the code correlation matrix is real and symmetric, and therefore the eigenvectors from different eigenvalues will be orthogonal [7,9].

The paper is organized as follows: Section II gives the system model used in the analysis. It also introduces the code correlation matrix. Section III presents the eigenstructure of the code correlation matrix. This section is really the crux of the method presented. Section IV presents the performance analysis together with the properties of the code correlation matrix. Section V presents the results and conclusion. The Appendix covers an example to illustrate results used in the derivations in the body of the paper.

II. System Model

The linear block codes considered here consist of codewords generated by a generator matrix and an information vector. The system is modelled as a binary phase-shift keying (PSK) with antipodal signalling and soft-decision decoding at the receiver. For some block codes selected for illustration, bit error rate results show remarkable agreement between simulations and analysis, and are a validation of the method.

Fig.1 depicts the signal flow incorporating the source encoder and channel. The output of the channel encoder is a set of bits $\mathbf{C}_{\mathbf{kj}}$, k=1,2,…,M, and j=1,2,…, n. This is then transformed so as to map binary 0's into –1, and binary 1's into +1, and the result is then multiplied by a positive scalar constant. The channel is modelled by an additive random variable $\mathbf{n}_\mathbf{j}$ which is assumed to be a sample of a zero-mean Gaussian noise process, and is therefore itself a zero-mean Gaussian random variable with variance $N_0/2$. The Gaussian assumption is made here for tractability of the analysis.

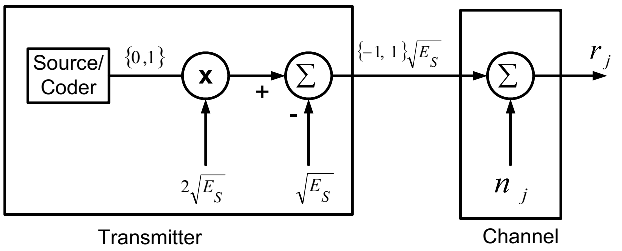

Fig. 1 Transmitter and channel to generate received symbols

In Fig.2 the receiver correlates the incoming signal $\mathbf{r}_\mathrm{j}$ with each codeword, and forms the decision variables $U_1, U_2, \ldots, U_M$ as shown. It then selects the largest of these to determine the transmitted codeword. Since the codes used are linear, the analysis assumes that the transmitted sequence corresponds to the all-zero codeword. The received symbol is therefore $r_j = n_j - \sqrt{E_S}$.

V. K. Oduol is with the Department of Electrical and Information Engineering, University of Nairobi, Nairobi, Kenya (+254-02-318262 ext.28327, vkoduol@uonbi.ac.ke)
Cemal Ardil is with the National Academy of Aviation, Baku, Azerbaijan

The correlation is achieved by multiplying the received symbol by $\left(2C_{ij}-1\right)\sqrt{E_S}$ and summing over all values of j.

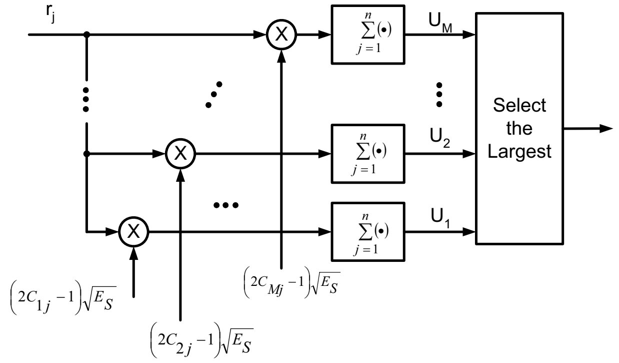
r_j
X
$\sum_{j=1}^{n}(\bullet)$
U_M
U_2
U_1
Select the Largest
$\left(2C_{1j}-1\right)\sqrt{E_S}$
$\left(2C_{2j}-1\right)\sqrt{E_S}$
$\left(2C_{Mj}-1\right)\sqrt{E_S}$

Fig. 2 The receiver forms the decision variables via correlation

The receiver forms the decision variables U_k as follows:

$$U_0 = nE_S - \left(\sqrt{E_S}\right)\sum_{j=1}^{n} n_j \tag{1}$$

$$U_k = \left(n-2w_k\right)E_S + \left(\sqrt{E_S}\right)\sum_{j=1}^{n}\left(2C_{kj}-1\right)n_j \quad \text{k=1,2,…,M} \tag{2}$$

where E_s is the signal energy. It is more convenient to work with the following decision variables

$$Z_k = \frac{1}{\sqrt{2E_S N_0}}\left(U_k - U_0\right) + w_k\sqrt{\frac{2E_S}{N_0}} \quad \text{k=1,2,…,M} \tag{3}$$

where $N_0/2$ is the power spectral density of the white noise. It can be shown that the mean and variance of Z_k are, respectively, $E\{Z_k\}=0$ and $\mathrm{Var}\{Z_k\} = w_k$. From the definition of U_k we have

$$Z_k = \left(\sqrt{2/N_0}\right)\sum_{j=1}^{n} C_{kj}\ n_j \tag{4}$$

A. Code Correlation Matrix

The correlation of the random variables Z_k and Z_l is

$$E\{Z_k, Z_l\} = \frac{2}{N_0}\sum_{j=1}^{n}\sum_{i=1}^{n} C_{kj}C_{li}\ E\{n_i\ n_j\} \tag{5}$$

Since the noise is presumed to be white, $E\{n_i\ n_j\} = \left(N_0/2\right)\delta_{ij}$, the correlation becomes

$$E\{Z_k, Z_l\} = \sum_{j=1}^{n} C_{kj}C_{lj} \ = r_{kl} \tag{6}$$

which is just the inner product of the two codewords $\mathbf{C}_k$ and $\mathbf{C}_l$. The code correlation matrix **R** is defined to have r_{kl} as its elements, with the diagonal elements equal to the weight of the kth codeword. That is, $r_{kk} = w_k$.

$$\mathbf{R} = \begin{pmatrix} w_2 & r_{23} & r_{24} & \cdots & r_{2M} \\ r_{32} & w_3 & r_{34} & \cdots & r_{3M} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ r_{M2} & r_{M3} & r_{M4} & \cdots & w_M \end{pmatrix} \tag{7}$$

The next section discusses the eigenvalue-eigenvector properties of the code correlation of (7).

III. EIGEN-STRUCTURE OF THE CODE CORRELATON MATRIX

For block codes, the code correlation matrix has the following properties.

Property 1: The weight vector of the code is an eigenvector with eigenvalue λ_1. That is $v_1 = \mathbf{w}$, and $\mathbf{Rw} = \lambda_1\mathbf{w}$. This eigenvalue has only one eigenvector, the weight vector. Incidentally λ_1 happens to be the largest eigenvalue, a fact not needed in the analysis addressed here, but found to be true in all the block codes examined.

Property 2: All other eigenvectors are orthogonal to the weight vector: $\mathbf{w}^{\mathbf{T}}\mathbf{v}_m = 0$, for $m \neq 1$. This follows from the fact the code correlation matrix is real and symmetric.

Property 3: Some eigenvalues may be zero; equivalently the null-space of the code correlation matrix may be non-empty.

Property 4: Except for λ_1, the other non-zero eigenvalues have eigenvectors with *zero-sum elements*. For the eigenvalue λ_m the corresponding eigenvector $\mathbf{v_k}$ has elements satisfying $v_{1,m,}+ v_{2,m} + \ldots + v_{M,m} = 0$.

The justifications for the first and last of these properties are provided next. The remaining two do not need justification beyond what is already stated.

A. The Weight Vector as an Eigenvector

The code correlation matrix is given by $\mathbf{R} = \mathbf{CC}^{\mathrm{T}}$. The weight vector is $\mathbf{w} = \mathbf{C1_n}$, where $\mathbf{1_n}$ is the n×1 vector of all ones. To show that the weight vector is an eigenvector of the code correlation matrix, it is considered that

$$(\mathbf{Rw})_m = \sum_{p=1}^{M}(\mathbf{R})_{mp}\, w_p \tag{8}$$

Using the fact that $(\mathbf{R})_{mp} = \sum_{j=1}^{n} C_{mj}C_{pj}$ and $w_p = \sum_{q=1}^{n} C_{pq}$ and substituting in (7) yields

$$\begin{aligned}(\mathbf{Rw})_m &= \sum_{p=1}^{M}\sum_{j=1}^{n} C_{mj}C_{pj}\sum_{q=1}^{n} C_{pq} \\ &= \sum_{j=1}^{n} C_{mj}\left(\sum_{q=1}^{n}\sum_{p=1}^{M} C_{pj}C_{pq}\right)\end{aligned} \tag{9}$$

where the order of summations has been changed in the last line. The inner-most sum (over p) is the inner product between column-j and column-q of the codeword array C.

When the index j is fixed, the sums (over p) are evaluated for each value of q, and added together from q = 1 to q = n. It turns out that the resulting sum in parentheses is the same, regardless of the value of j. This is observed to hold for all the linear codes examined in this work. The value of this sum is λ_1, the eigenvalue for the weight vector. Accordingly,

$$\lambda_1 = \left(\sum_{q=1}^{n}\sum_{p=1}^{M} C_{pj}C_{pq}\right) \tag{10}$$

where j is any legitimate column index. With this result the expression in (8) becomes

$$(\mathbf{Rw})_m = \lambda_1\sum_{j=1}^{n} C_{mj} = \lambda_1 w_m \tag{11}$$

from which it is evident that

$$\mathbf{Rw} = \lambda_1\mathbf{w} \tag{12}$$

indicating that the weight vector is an eigenvector of the code correlation matrix, with λ_1 as the corresponding eigenvalue. The expression in (10) for the eigenvalue consists of two nested sums. The inner sum is found to equal 2^{k-1} for q = j, and to equal 2^{k-2} for the remaining n - 1 values of q. This is found to hold for all the linear block codes examined in this pape*r*. Of course it can be proved by using the generator matrix of the code and the information sequences used to create the code array. The present paper omits that exercise, and instead uses the observations made from the codes examined. The total in (10) is $2^{k-1} + 2^{k-2}$ (n-1), which gives

$$\lambda_1 = 2^{k-2}(n+1) \tag{13}$$

Thus, the eigenvalue depends only on *n* and *k*, which are the two code parameters.

B. Other Non-Zero Eigenvalues

As before $\mathbf{v}_m = \mathbf{C}\boldsymbol{x}$ is any any of the eigenvectors corresponding to λ_m for m ≠1 with the vector $\boldsymbol{x}$ being n×1. In a parallel development to the case for the weight vector,

$$(\mathbf{RCx})_m = \sum_{p=1}^{M} (\mathbf{R})_{mp} (\mathbf{Cx})_p \tag{14}$$

Using the fact that $(\mathbf{R})_{mp} = \sum_{j=1}^{n} C_{mj} C_{pj}$ and $(\mathbf{Cx})_p = \sum_{q=1}^{n} C_{pq} x_q$ and substituting in (14) yields

$$\begin{aligned}(\mathbf{R}v)_m &= \sum_{p=1}^{M}\sum_{j=1}^{n} C_{mj} C_{pj} \sum_{q=1}^{n} C_{pq} x_q \\ &= \sum_{j=1}^{n} C_{mj} \sum_{q=1}^{n} x_q \left(\sum_{p=1}^{M} C_{pj} C_{pq} \right)\end{aligned} \tag{15}$$

The inner-most sum (over p) has appeared before; it equals 2^{k-1} for q = j and equals 2^{k-2} for q ≠ j.

$$(\mathbf{R}v)_m = 2^{k-2} \sum_{j=1}^{n} C_{mj} \left(2x_j + \sum_{q \neq 1}^{n} x_q \right) \tag{16}$$

This can be re-written as

$$(\mathbf{R}v)_m = 2^{k-2} \sum_{j=1}^{n} C_{mj} \left(x_j + \sum_{q=1}^{n} x_q \right) \tag{17}$$

The sum over q has been shown to be zero, and therefore

$$(\mathbf{R}v)_m = 2^{k-2} \sum_{j=1}^{n} C_{mj} x_j \tag{18}$$

The right hand side is seen to represent the m-th component of **Cv, i.e.** the m-th component of the eigenvector, **v**. This leads to the result ***Rv*** = *kv*, which says that the non-zero eigenvalue sought is

$$\lambda_m = 2^{k-2} \qquad m \neq 1 \tag{19}$$

The eigenvalue obtained in (13) is n+1 times λ_m. Since n > 1 a comparison of (19) with (13) shows that λ_1 corresponding to the weight vector the largest eigenvalue of the code correlation matrix.

C. Zero-Sum Eigenvectors

Since the code correlation matrix is real and symmetric, the eigenvectors $\mathbf{v}_m$ corresponding to λ_m with m ≠ 1 are orthogonal to the weight vector. For the presentation here the vector $\mathbf{C}\boldsymbol{x}$ represents any of the eigenvectors $\mathbf{v}_m$, where the vector $\boldsymbol{x}$ is n×1.

$$\begin{aligned} 0 = (\mathbf{Cx})^T \mathbf{W} &= \sum_{p=1}^{M}\sum_{j=1}^{n} x_j C_{pj} \sum_{q=1}^{n} C_{pq} \\ &= \sum_{j=1}^{n} x_j \left(\sum_{q=1}^{n} \sum_{p=1}^{M} C_{pj} C_{pq} \right)\end{aligned} \tag{20}$$

The double sum in parentheses in (20) brackets has been shown to equal λ_1, independent of j. Thus

$$\sum_{j=1}^{n} x_j = 0 \tag{21}$$

an intermediate result which will be used shortly. Continuing these proceedings, the sum of the elements of this vector is

$$\sum_{p=1}^{M} (\mathbf{Cx})_p = \sum_{p=1}^{M}\sum_{j=1}^{n} C_{pj} x_j \tag{22}$$

Changing the order of summations gives

$$\sum_{p=1}^{M} (\mathbf{Cx})_p = \sum_{j=1}^{n} x_j \left(\sum_{p=1}^{M} C_{pj} \right) \tag{23}$$

At this point it is important once again to invoke an observed result form the code array, that the sum in parentheses is the sum of the elements in column-j of the code array. This sum is found to be a constant independent of j. In fact, it is found to equal 2^{k-1}, where k is the number of information bits in the n-bit codeword. As noted previously in connection with (10) here too it is possible to prove this using the generator matrix of the code and the information sequences used to generate the codewords. For the same reason given earlier, the paper uses the observations made on the linear codes examined.

$$\sum_{p=1}^{M} v_{p,m} = k \sum_{j=1}^{n} x_j \tag{24}$$

The sum on the right has been shown in (21) to be zero. Therefore

$$\sum_{p=1}^{M} v_{p,m} = 0 \tag{25}$$

which shows that the eigenvectors belonging to the non-zero eigenvalue λ_m for m ≠1 have zero-sum elements. That is the elements sum to zero.

D. Number of Zero-Sum Eigenvectors

The weight vector is the only vector corresponding to the eigenvalue λ_1. As for the other non-zero eigenvalues the condition in (21) involves n variables. This means that there are n-1 free variables, and therefore n-1 eigenvectors corresponding to the eigenvalue λ_m for m ≠1. Specifically the expression in (21) can be used to obtain the eigenvectors as

$$\mathbf{Cx} = \mathbf{C}\begin{pmatrix}1\\0\\0\\\vdots\\-1\end{pmatrix}, \mathbf{C}\begin{pmatrix}0\\1\\0\\\vdots\\-1\end{pmatrix}, \mathbf{C}\begin{pmatrix}0\\0\\1\\\vdots\\-1\end{pmatrix}, \cdots, \mathbf{C}\begin{pmatrix}0\\\vdots\\0\\1\\-1\end{pmatrix} \tag{26}$$

This says that the eigenvectors are obtained by subtracting the last column of the code array from each of the first n-1 columns of the code array **C**. It is noted that while (26) uses the last column of the code array to create the n-1 vectors, any one column could have been used. The same set of vectors will be obtained, although in a different order.

These together with the weight vector constitute a total of n eigenvectors. Since the code correlation matrix is M×M, where $M = 2^k - 1$, a total of M vectors is required. The remaining (M – n) vectors must come from the null space of the code correlation matrix. While it is possible to obtain expression for the vectors in null space of the code correlation matrix, this is not addressed here since it is not needed in meeting the present objectives. These vectors from the null space can be transformed by the Gram-Schmidt process [7-9] if necessary, to make them orthogonal to the vectors already obtained, and also to be mutually orthogonal themselves.

This completes the discussion of the eigen-structure of the code correlation matrix for the purposes of the paper. It is now possible to return to the issue of analyzing the performance of the block codes under the scenario described previously in Section II.

IV. PERFORMANCE ANALYSIS

Referring to (1) and (2) and assuming that the transmitted codeword is the all-zero codeword, the receiver makes the correct decision if and only if $U_{\mathbf{k}} - U_{\mathbf{0}} < 0$, for k=1,3, …,M, a requirement which together with (3) translates to

$$Z_k < w_k\sqrt{\frac{2E_S}{N_0}} \quad \text{for } k=1,2, \ldots,M. \tag{27}$$

The event of a correct symbol detection corresponds to the joint event $E_1 \cap < E_2 \cap \cdots \cap E_M$ where

$$E_k = \left(-\infty < Z_k < w_k\right) \quad k=1,2,\ldots,M \tag{28}$$

A. Transformation of the Decision Variables

The analysis would be easier when the events are disjoint, which is achieved by applying a unitary transformation to the space of the random variables $Z_1, Z_2, \ldots, Z_M$. The transformation of random variables to facilitate analysis is employed in many texts [8,10]. Under the transformation, the two points $(-\infty, -\infty, -\infty, \ldots, -\infty)^T$ and $(w_1, w_2, w_3, \ldots w_M)^T$ will be mapped into new image points. To this send the following transformation is applied

$$\mathbf{X} = \mathbf{V}^T\mathbf{Z} \tag{29}$$

where **V** is the matrix of eigenvectors selected to have orthornormal columns. That is

$$\mathbf{V}^T\mathbf{V} = \mathbf{I} \tag{30}$$

To determine the image of the two points referred to above, it is considered that the first vector in the matrix **V** is the normalized weight vector $\mathbf{v}_1 = \mathbf{w}/||\mathbf{w}||$, and all the other vectors in **V** are orthogonal to **w.** Accordingly the image of the point $(w_1, w_2, w_3, \ldots w_M)^T$ will be $(||\mathbf{w}||, 0, 0, \ldots, 0)^T$. For the other point the limit $\lim\limits_{B\to-\infty}\{B(w_1, w_2, \cdots, w_M)\}$ is considered, which gives the image as $\lim\limits_{B\to-\infty}\left\{B\left(\|\mathbf{w}\|, 0, \cdots, 0\right)\right\}$, using the fact that the other vectors in **V** are orthogonal to the weight vector.

It must be stated immediately here that the results obtained later by this consideration are found to be in agreement with those found by simulation. When the limit is taken, the image of the point in question is seen to be $(-\infty, 0, 0, \ldots, 0)^T$.

The random variables $Z_1, Z_2, \ldots, Z_M$ are zero-mean and jointly Gaussian in distribution. In such cases the result of the transformation in (29) would normally be a new set of random variables $X_1, X_2, \ldots, X_M$ which are statistically independent, and with a Gaussian distribution, given that the original set is Gaussian. Here the situation is much simpler, in that the transformation has produced the mapping as shown in Fig.3

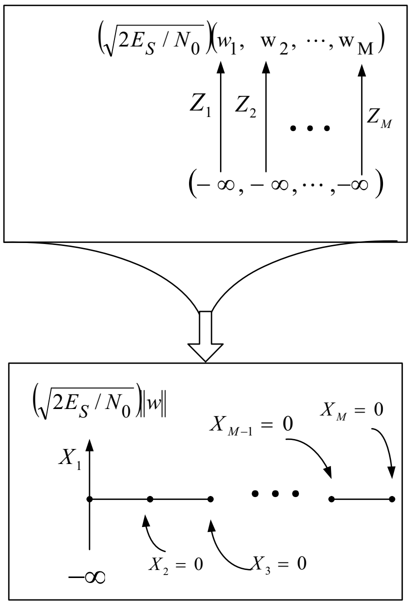
$\left(\sqrt{2E_S/N_0}\right)(w_1, w_2, \cdots, w_M)$
Z_1
Z_2
Z_M
$(-\infty, -\infty, \cdots, -\infty)$
$\left(\sqrt{2E_S/N_0}\right)\|w\|$
X_1
$X_{M-1} = 0$
$X_M = 0$
$-\infty$
$X_2 = 0$
$X_3 = 0$

Fig. 3 Mapping of the Limits

In the upper part of the figure the variables Z_1 Z_2,..,Z_M each varies as shown by the arrows. In the lower part of the figure only X_1 varies (as shown by the arrow); the other variables X_2, $X_{3\ldots}$,X_M have collapsed to zero. Therefore the result of the transformation is to produce one random variable X_1, and reduce the others to probability masses at zero.

B. Probability of Correct Symbol

The probability of correct symbol is then given by

$$P_{CW} = \Pr\left\{-\infty < X_1 \le \|w\|\sqrt{2E_S/N_0}\right\} \tag{31}$$

The original set of random variables are each Gaussian by assumption. Therefore since the transformation is linear, the resulting random variables should also be Gaussian. Here only one random variable results. The variance of this random variable is the eigenvalue corresponding to the largest eigenvalue λ_1 of the code correlation matrix. Accordingly the probability of correct symbol is found to be

$$P_{CW} = \frac{1}{\sqrt{2\pi\lambda_1}}\int_{-\infty}^{\|w\|\sqrt{2E_S/N_0}} \exp\left(-\frac{y^2}{2\lambda_1}\right)dy \tag{32}$$

By an appropriate change of variable, this can be expressed as

$$P_{CW} = \frac{1}{2} + \frac{1}{2}erf\left(\sqrt{\frac{\|w\|^2 E_S}{\lambda_1 N_0}}\right) = 1 - \frac{1}{2}erfc\left(\sqrt{\frac{\|w\|^2 E_S}{\lambda_1 N_0}}\right) \tag{33}$$

where erf(x) and erfc(x) are the error function and the complementary error function, respectively.

C. Bit Error Probability

Since a word consists of n bits, an estimate of the bit error probability P_b can be can be obtained from P_{CW} by using

$$P_b = 1-\left(P_{CW}\right)^{1/n} \tag{34}$$

where n is the nmber of bits in a codeword.

V. RESULTS AND CONCLUSION

Fig.4 shows results for the correct symbol probabilities for the (7,4,3) BCH code. One set is obtained via simulation (diamonds) and the other via analysis (solid line). These are in the upper part of the figure. Also provided are the corresponding results for the uncoded symbols. It is observed that there is agreement between the results from simulation and analysis. Needless to say, the results obtained via coding are better than those without.

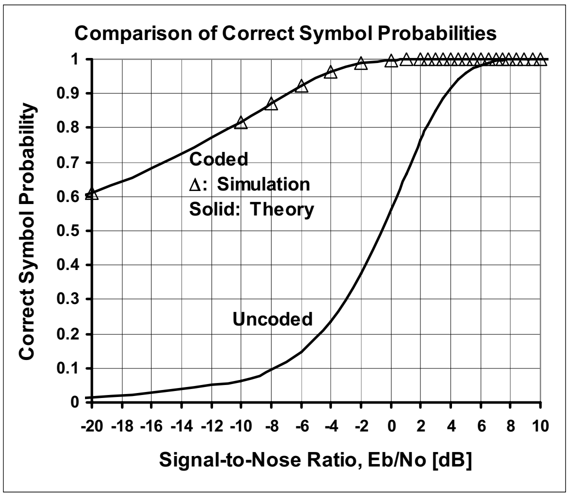

Fig. 4. Comparison of correct symbol probabilities

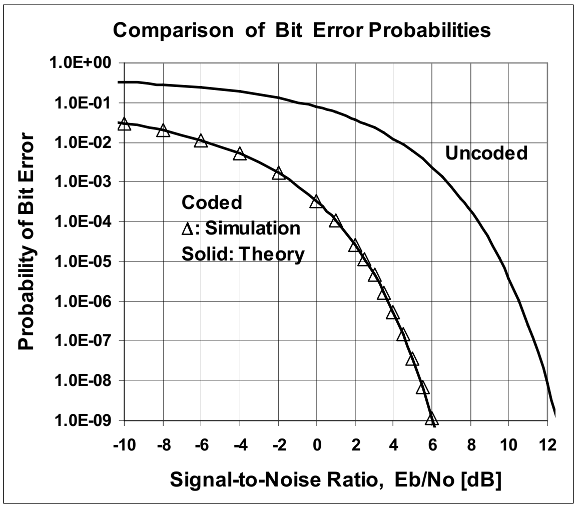

Fig. 5. Comparison of bit error probabilities

Fig.5 gives a comparison of bit error probabilities using results from simulation, analysis, and uncoded symbols. Again, the simulation and anlysis results exhibit agreement. The uncoded symbol results (upper trace) indicate a higher bit error probability than the ones obtained by coding.

This work has presented a method of computing the error probability for a block code using the eigenvalue-eigenvector structure of the code correlation matrix. It is found that there is one largest eigenvalue whose only eigenvector is the weight vector. The other eigenvectors have elements that add up to zero.

The largest eigenvalue and its eigenvector (the weight vector) are used to determine the symbol error probability of a block code using BPSK and soft-decision decoding. A comparison of the simulation and analysis results provides validation of the analysis presented.

APPENDIX

The codewords are arranged in rows to form the matrix **C** as given below.

$$\mathbf{C} = \begin{pmatrix} C_{1,1},\ C_{1,2},\ \cdots,\ C_{1,n} \\ C_{2,1},\ C_{2,2},\ \cdots,\ C_{2,n} \\ \vdots \\ C_{M,1}, C_{M,2}, \cdots, C_{M,n} \end{pmatrix} \tag{34}$$

In this array, the all-zero codeword is not sown. As an illustration the (7,4,3) BCH code with generator matrix G

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{35}$$

has the codewords given in Table I

TABLE I CODEWORDS OF THE (7,4,3) BCH CODE

Index	codeword							weight
1	0	0	0	1	1	0	1	3
2	0	0	1	0	1	1	1	4
3	0	0	1	1	0	1	0	3
4	0	1	0	0	0	1	1	3
5	0	1	0	1	1	1	0	4
6	0	1	1	0	1	0	0	3
7	0	1	1	1	0	0	1	4
8	1	0	0	0	1	1	0	3
9	1	0	0	1	0	1	1	4
10	1	0	1	0	0	0	1	3
11	1	0	1	1	1	0	0	4
12	1	1	0	0	1	0	1	4
13	1	1	0	1	0	0	0	3
14	1	1	1	0	0	1	0	4
15	1	1	1	1	1	1	1	7

and the code correlation matrix is given by the array shown in Fig.6. The elements of the weight vector appear as the diagonal elements in the matrix. The matrix is seen to be symmetric and has real elements.

Through other methods of determining the eigenvalue, and it can be established that the largest eigenvalue is 32, and the other non-zero eigenvalue is 4. These agree with (13) and (19), respectively. That is $\lambda_1 = (7+1)\times 2^{4-2} = 32$ and $\lambda_m = 2^{4-2} = 4$. form $m \neq 1$..

Other codes are given below so as to enable comparisons and validation of some the expressions given in the analysis. The example of the (3,2,2) code is simple enough that the results can be checked very quickly, without much effort. The other example is (6,3,3) code.

3	2	1	1	2	1	2	1	2	1	2	2	1	0	3
2	4	2	2	2	2	2	2	2	2	2	2	0	2	4
1	2	3	1	2	1	2	1	2	1	2	0	1	2	3
1	2	1	3	2	1	2	1	2	1	0	2	1	2	3
2	2	2	2	4	2	2	2	2	0	2	2	2	2	4
1	2	1	1	2	3	2	1	0	1	2	2	1	2	3
2	2	2	2	2	2	4	0	2	2	2	2	2	2	4
1	2	1	1	2	1	0	3	2	1	2	2	1	2	3
2	2	2	2	2	0	2	2	4	2	2	2	2	2	4
1	2	1	1	0	1	2	1	2	3	2	2	1	2	3
2	2	2	0	2	2	2	2	2	2	4	2	2	2	4
2	2	0	2	2	2	2	2	2	2	2	4	2	2	4
1	0	1	1	2	1	2	1	2	1	2	2	3	2	3
0	2	2	2	2	2	2	2	2	2	2	2	2	4	4
3	4	3	3	4	3	4	3	4	3	4	4	3	4	7

Fig. 6 Elements of the code correlation matrix for the (7,4,3) BCH Code

The (3,2,2) code has the non-zero codewords given in Table II,

TABLE II CODEWORDS OF THE (3,2,2) CODE

Index	codeword			weight
1	0	1	1	2
2	1	0	1	2
3	1	1	0	2

and the code correlation matrix

$$R = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}. \tag{36}$$

The eigenvalues of this matrix are easily computed, and verified from the text, using k = 2 and n = 3 in(13) and (19), to be $\lambda_1 = 4$ and $\lambda_2 = 1$. The corresponding eigenvectors, already orthonormalized are found to be

$$\mathbf{v}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathbf{v}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathbf{v}_3 = \frac{1}{\sqrt{6}}\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \tag{37}$$

Table III gives codewords of the (6,3,3) code and their weight respective weights

TABLE III CODEWORDS OF THE (6,3,3) BCH CODE

Index	codeword						weight
1	0	0	1	0	1	1	3
2	0	1	0	1	1	0	3
3	0	1	1	1	0	1	4
4	1	0	0	1	0	1	3
5	1	0	1	1	1	0	4
6	1	1	0	0	1	1	4
7	1	1	1	0	0	0	3

The code correlation matrix of this code is found to be

3	1	2	1	2	2	1
1	3	2	1	2	2	1
2	2	4	2	2	2	2
1	1	2	3	2	2	1
2	2	2	2	4	2	2
2	2	2	2	2	4	2
1	1	2	1	2	2	3

Fig.7 Elements of the code correlation matrix for the (6,3,3) Code

The non-zero eigenvalues are found to be $\lambda_1 = 14$ and $\lambda_2 = 2$. with the eigenvalectors

$$\frac{1}{2\sqrt{21}}\begin{pmatrix} 3 \\ 3 \\ 4 \\ 3 \\ 4 \\ 4 \\ 3 \end{pmatrix}, \quad \frac{1}{2}\begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad \frac{1}{2}\begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \\ 1 \\ -1 \\ 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \quad \frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{38}$$

There is one vector left, that needs to come from the null-space of the code correlation matrix. It is observed that the first vector (parallel to the weight vector) is orthogonal to each of the others. Also the vectors are *not mutually orthogonal*, *and will need the Gram-Schmidt process*. The codes, their code correlation matrices and the corresponding eigen-structures are given in this Appendix to provide a means to verify the findings of the work.

REFERENCES

[1] Shu Lin and Daniel J. Costello, Jr., *Error Control Coding: Fundamentals and Applications,* Prentice Hall: Englewood Cliffs, NJ, 1983.

[2] A. M. Michelson and A. H. Levesque, "Error-Control Techniques for Digital Communication", *a Wiley-Interscience Publication*, 1985

[3] W.W. Peterson and E.J. Weldon, Jr., *Error-Correcting Codes*, 2nd edition, MIT Press: Cambridge, Mass., 1972.

[4] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland: New York, NY, 1977.

[5] E. R. Berlekamp, R. E. Peile, and S. P. Pope, "*The Application of Error Control to Communications*," IEEE Communications Magazine., Vol. 25, pp. 44–57, 1987.

[6] Wicker, Stephen B., *Error Control Systems for Digital Communication and Storage*, Upper Saddle River, N.J., Prentice Hall, 1995.

[7] S. Haykin, *Adaptive Filter Theory,* 4th Edition, *(*Appendix E. Eigenanalysis*)*, Prentice Hall 2001

[8] S. Haykin, *Communication Systems,* 4th Edition, John Wiley & Sons 2001

[9] G.H. Golub, C.F. Van Loan, *Matrix Computations, 3rd ed.* Johns Hopkins, 1996.

[10] J.G. Proakis, *Digital Communications*, 3rd Ed, McGraw-Hill, 1995.

Vitalice K. Oduol received his pre-university education at Alliance High School in Kenya. In 1981 he was awarded a CIDA scholarship to study electrical engineering at McGill University, Canada, where he received the B.Eng. (Hons.) and M.Eng. degrees in 1985 and 1987, respectively, both in electrical engineering. In June 1992, he received the Ph.D. degree in electrical engineering at McGill University.

He was a research associate and teaching assistant while a graduate student at McGill University. He joined MPB Technologies, Inc. in 1989, where he participated in a variety of projects, including meteor burst communication systems, satellite on-board processing, low probability of intercept radio, among others. In 1994 he joined INTELSAT where he initiated research and development work on the integration of terrestrial wireless and satellite systems. After working at COMSAT Labs. (1996-1997) on VSAT networks, and TranSwitch Corp.(1998-2002) on product definition and architecture, he returned to Kenya, where since 2003 he has been with Department of Electrical and Information Engineering, University of Nairobi.

Dr. Oduol was a two-time recipient of the Douglas tutorial scholarship at McGill University. He is currently chairman, Department of Electrical and Information Engineering, University of Nairobi. His research interests include performance analysis, modeling and simulation of telecommunication systems, adaptive error control, feedback communication.

Cemal Ardil is with the National Academy of Aviation, Baku, Azerbaijan