A BPSK Model for Soft-Output Decoding of Binary Linear Block Codes

Pragat Chaudhari and Amir K. Khandani

Dept. of Elec. and Comp. Engineering

University of Waterloo

Waterloo, Ontario N2L 3G1

pragat@shannon.uwaterloo.ca khandani@shannon.uwaterloo.ca

Tel. (519) 885-1211 x5324, Fax. (519) 746-3077

Abstract—**It is shown that the bit LLR value in soft-output decoding of a binary linear block code with BPSK modulation can be closely modeled by a second BPSK modulation of reduced noise power. With this modeling, it is possible to provide bit error performance approximations to help in the evaluation of binary linear codes. This can also be used in the design of communications systems which require knowledge of the characteristics of the channel, such as combined source-channel coding. Simulation results are presented which show that the actual bit error performance of the code is very well approximated by this modeling, especially for low signal-to-noise ratios (SNR). Furthermore, arguments are presented which show that the approximation requires fewer samples than conventional simulation methods to obtain the same precision in the bit error probability value. This translates into fewer computations and therefore, less time is needed to obtain performance results.**

I. Introduction

Assume that a binary linear code $\mathcal{C}$ is given, and the codewords $\boldsymbol{c}_j$, $j = 1, 2, \ldots, |\mathcal{C}|$, are BPSK modulated to values of $\pm$ 1. The received codeword is denoted by $\boldsymbol{x} = \tilde{\boldsymbol{c}} + \boldsymbol{\eta}$, where $\tilde{\boldsymbol{c}}$ is the transmitted (modulated) codeword and $\boldsymbol{\eta}$ is the vector of Additive White Gaussian Noise (AWGN) with mean 0 and variance σ_η^2. The LLR of bit k of the transmitted (binary) codeword $\boldsymbol{m}$ can be computed using,

$$
\begin{aligned}
LLR(m_k) &= \log \frac{\Pr(m_k = 1|\boldsymbol{x})}{\Pr(m_k = 0|\boldsymbol{x})} \\
&= \log \frac{\sum_{\boldsymbol{c}_i \,\epsilon\, \mathcal{C}_1} \exp\{-\frac{||\boldsymbol{x}-\boldsymbol{c}_i||^2}{2\sigma_\eta^2}\}}{\sum_{\boldsymbol{c}_j \,\epsilon\, \mathcal{C}_0} \exp\{-\frac{||\boldsymbol{x}-\boldsymbol{c}_j||^2}{2\sigma_\eta^2}\}} \\
&= \log \frac{\sum_{\boldsymbol{c}_i \,\epsilon\, \mathcal{C}_1} \exp\{\frac{\boldsymbol{x}\cdot\boldsymbol{c}_i}{\sigma_\eta^2}\}}{\sum_{\boldsymbol{c}_j \,\epsilon\, \mathcal{C}_0} \exp\{\frac{\boldsymbol{x}\cdot\boldsymbol{c}_j}{\sigma_\eta^2}\}} \\
&= \log\Bigg(\sum_{\boldsymbol{c}_i \,\epsilon\, \mathcal{C}_1} \exp\{\frac{\boldsymbol{\eta}\cdot\boldsymbol{c}_i + \tilde{\boldsymbol{c}}\cdot\boldsymbol{c}_i}{\sigma_\eta^2}\}\Bigg) \\
&\quad - \log\Bigg(\sum_{\boldsymbol{c}_j \,\epsilon\, \mathcal{C}_0} \exp\{\frac{\boldsymbol{\eta}\cdot\boldsymbol{c}_j + \tilde{\boldsymbol{c}}\cdot\boldsymbol{c}_j}{\sigma_\eta^2}\}\Bigg) \qquad (1) \\
&= f(\boldsymbol{\eta}) - g(\boldsymbol{\eta}) \qquad (2)
\end{aligned}
$$

where, $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by dividing the code $\mathcal{C}$ into two groups based on the value of the bit in position k. Note that $\mathcal{C}_0$ is a sub-code and $\mathcal{C}_1$ is its coset. Given the value of the LLR, the decision on bit m_k is made by comparing the LLR with a threshold of zero.

This work was financially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and by Communications and Information Technology Ontario (CITO).

A more detailed version of this work can be found in [1, 2].

We are interested in studying the probabilistic behaviour of the LLR as a function of the Gaussian random vector $\boldsymbol{\eta}$. As we will see in the following theorems, the choice of $\tilde{\boldsymbol{c}}$ does not have any impact on the resulting probability distribution, assuming a linear code. To carry out the proofs, we need to assume that the noise is symmetrical about the origin. This is the case for the Gaussian probability density function.

Theorem 1: The probability distribution of $LLR(m_k)$ is not affected by the choice of $\tilde{\boldsymbol{c}}$ as long as the value of the bit k remains unchanged.

Proof: This can be proven using the distance invariance property of the code and the assumed symmetrical nature of the noise probability density function about zero [1, 2]. ∎

Theorem 2: The probability distribution of $LLR(m_k)$ for $m_k = 0$ and $m_k = 1$ are the reflections of one another through the origin (threshold point).

Proof: The distance invariance property and the symmetry of the noise probability density function can be used here again [1, 2]. ∎

Noting the above theorems, we assume that the all-zero codeword, denoted as $\boldsymbol{c}_0 = \mathbf{-1} \equiv (-1, -1, \ldots, -1)$, is transmitted in all our following discussions for convenience.

We use the notation $H(\boldsymbol{\eta})$ to refer to the LLR expression above. The Taylor series expansion of $H(\boldsymbol{\eta})$ around vector zero, $\mathbf{0} = (0, 0, \ldots, 0)$, is formulated using the expression below [3] in powers of η.

$$
\begin{aligned}
H(\boldsymbol{\eta}) &= H(\mathbf{0}) + \boldsymbol{\eta}\cdot\nabla H(\mathbf{0}) + \frac{1}{2}(\boldsymbol{\eta}\cdot\nabla)^2 H(\mathbf{0}) + \ldots \\
&= H(\mathbf{0}) + \sum_{p=1}^{n} \frac{\partial}{\partial\eta_p} H(\mathbf{0})\,\eta_p + \frac{1}{2}\sum_{v=1}^{n} \frac{\partial^2}{\partial\eta_v^2} H(\mathbf{0})\,\eta_v^2 \\
&\quad + \sum_{p\neq q,\, p<q\le n}^{n}\sum^{n} \frac{\partial}{\partial\eta_p}\frac{\partial}{\partial\eta_q} H(\mathbf{0})\,\eta_p\,\eta_q + \ldots \qquad (3)
\end{aligned}
$$

The expressions of $H(\mathbf{0})$ can be replaced with the expressions of $f(\boldsymbol{\eta})$ and $g(\boldsymbol{\eta})$ to simplify the expansion. The expansion is carried forward to the second-order using (3).

To simplify the expressions, the following weight enumeration functions are defined. Since the codewords are modulated to ± 1, their weights are denoted by the exponent $2w-n$ below, where n is the length of the codewords. We define,

$$A^{\mathcal{C}_i}(Z) = \sum_{w=0}^{n} A_w^{\mathcal{C}_i} Z^{2w-n} \tag{4}$$

where, $\mathcal{C}_i = \mathcal{C}_0$ or $\mathcal{C}_1$, $A_w^{\mathcal{C}_i}$ is the number of codewords of Hamming weight w in $\mathcal{C}_i$, and $Z = \exp\{-\frac{1}{\sigma_\eta^2}\}$. We also define,

$$B^{\mathcal{C}_i}(Z,p,\alpha) = \sum_{w=0}^{n} B_w^{\mathcal{C}_i}(p,\alpha)\, Z^{2w-n} \tag{5}$$

where $\mathcal{C}_i = \mathcal{C}_0$ or $\mathcal{C}_1$ and $B_w^{\mathcal{C}_i}(p,\alpha)$ is the number of codewords in $\mathcal{C}_i$ with Hamming weight w, for which the bit p is equal to $\alpha = 0, 1$.

With these definitions, the expansion is expressible as,

$$\begin{aligned} LLR(m_k) &= \log\left(\frac{A^{\mathcal{C}_1}(Z)}{A^{\mathcal{C}_0}(Z)}\right) \\ &+\frac{1}{\sigma_\eta^2}\sum_{p=1}^{n}\Bigg[\frac{[B^{\mathcal{C}_1}(Z,p,1)-B^{\mathcal{C}_1}(Z,p,0)]}{A^{\mathcal{C}_1}(Z)} \\ &\qquad - \frac{[B^{\mathcal{C}_0}(Z,p,1)-B^{\mathcal{C}_0}(Z,p,0)]}{A^{\mathcal{C}_0}(Z)}\Bigg]\eta_p \\ &+\frac{1}{2\sigma_\eta^4}\sum_{v=1,v\neq k}^{n}\Bigg[\Bigg[1-\frac{\left(B^{\mathcal{C}_1}(Z,v,1)-B^{\mathcal{C}_1}(Z,v,0)\right)^2}{\left(A^{\mathcal{C}_1}(Z)\right)^2}\Bigg] \\ &\qquad -\Bigg[1-\frac{\left(B^{\mathcal{C}_0}(Z,v,1)-B^{\mathcal{C}_0}(Z,v,0)\right)^2}{\left(A^{\mathcal{C}_0}(Z)\right)^2}\Bigg]\Bigg]\eta_v^2 \\ &+\frac{1}{\sigma_\eta^4}\sum_{\substack{p=1\\ p\neq q, p<q\leq n,\ p,q\neq k}}^{n}\sum_{q=1}^{n}(F-G)\,\eta_p\,\eta_q \end{aligned} \tag{6}$$

where, F and G are defined as

$$\begin{aligned} F = &\frac{B^{\mathcal{C}_1}(Z,p\oplus q,1)-B^{\mathcal{C}_1}(Z,p\oplus q,0)}{A^{\mathcal{C}_1}(Z)} \\ &-\frac{\left(B^{\mathcal{C}_1}(Z,p,1)-B^{\mathcal{C}_1}(Z,p,0)\right)\left(B^{\mathcal{C}_1}(Z,q,1)-B^{\mathcal{C}_1}(Z,q,0)\right)}{\left(A^{\mathcal{C}_1}(Z)\right)^2} \end{aligned} \tag{7}$$

$$\begin{aligned} G = &\frac{B^{\mathcal{C}_0}(Z,p\oplus q,1)-B^{\mathcal{C}_0}(Z,p\oplus q,0)}{A^{\mathcal{C}_0}(Z)} \\ &-\frac{\left(B^{\mathcal{C}_0}(Z,p,1)-B^{\mathcal{C}_0}(Z,p,0)\right)\left(B^{\mathcal{C}_0}(Z,q,1)-B^{\mathcal{C}_0}(Z,q,0)\right)}{\left(A^{\mathcal{C}_0}(Z)\right)^2}, \end{aligned} \tag{8}$$

The above expression of (6) can be simplified as,

$$\begin{aligned} LLR(m_k) = K_0 &+ \frac{1}{\sigma_\eta^2}\sum_{p=1}^{n}K_1(p)\eta_p + \left(\frac{1}{\sigma_\eta^2}\right)^2\Bigg(\sum_{v=1,v\neq k}^{n}K_2(v)\eta_v^2 \\ &+ \sum_{\substack{p=1\\ p\neq q, p<q\leq n,\ p,q\neq k}}^{n}\sum_{q=1}^{n}K_3(p,q)\,\eta_p\,\eta_q\Bigg) + \ldots . \end{aligned} \tag{9}$$

The constants K_0, K_1, K_2, and K_3 are all expressible in terms of the weight distributions of $\mathcal{C}_0$ and $\mathcal{C}_1$, and are straightforward to calculate.

The expression of (9) is composed of summations of random variables. The term K_0 is simply a constant dependent on the weight distribution of the code. The first-order terms are a summation of scaled and independent Gaussian random variables (RV) yielding a Gaussian RV for the sum. Higher-order terms can be organized into groups such that the sum of the RV of the group can be approximated by a Gaussian RV, for large enough n by the Central Limit Theorem. For example, the second-order terms can be grouped as $\{\eta_1^2, \eta_2^2, \ldots, \eta_n^2\}$, $\{\eta_1\eta_2, \eta_3\eta_4, \ldots, \eta_{n-1}\eta_n\}$, and $\{\eta_2\eta_3, \eta_4\eta_5, \ldots, \eta_n\eta_1\}$. The groupings exhibit a Gaussian distribution, although not independent of one another, however, their sum can be approximated to be Gaussian.

Similar groupings can be formed for even higher-order terms, however, due to fewer unique product terms among the n elements, the Gaussian approximation cannot be applied. However, the following theorem can be used to argue that these terms are not as important.

Theorem 3: The higher-order partial derivative coefficients in the expansion of $f(\boldsymbol{\eta})$ approach 0 as the noise variance, σ_η^2, approaches infinity.

Proof: The coefficients of the series are formed with partial derivatives and subsequently, setting $\boldsymbol{\eta} = \mathbf{0}$. By induction, it can be shown [1, 2] that the $k+1^{st}$ partial derivative of $f(\boldsymbol{\eta})$, assuming that, without loss of generality, the $k+1^{st}$ partial derivative is taken with respect to η_1, is given by

$$\begin{aligned} \frac{\partial^{k+1} f}{\partial\eta_1^{m_1+1}\partial\eta_2^{m_2}\ldots\partial\eta_n^{m_n}} &= e^{-f}\frac{\partial^{k+1} A}{\partial\eta_1^{m_1+1}\partial\eta_2^{m_2}\ldots\partial\eta_n^{m_n}} \\ &-e^{-f}\frac{\partial}{\partial\eta_1}\left(e^f X_k\right) - \frac{\partial^k f}{\partial\eta_1^{m_1}\partial\eta_2^{m_2}\ldots\partial\eta_n^{m_n}}\frac{\partial f}{\partial\eta_1} \end{aligned} \tag{10}$$

where, $m_1 + m_2 + \ldots + m_n = k$; A is defined as

$$A = e^{f(\boldsymbol{\eta})} = \sum_{\boldsymbol{c}_i \in \mathcal{C}_1}\exp\{\frac{\boldsymbol{\eta}\cdot\boldsymbol{c}_i + \tilde{\boldsymbol{c}}\cdot\boldsymbol{c}_i}{\sigma_\eta^2}\}; \tag{11}$$

and X_k is composed of lower-order partial derivatives of $f(\boldsymbol{\eta})$. Repeated differentiation of A yields a multiplicative factor of $1/\sigma_\eta^2$ and the multiplication of the appropriate codeword component with each partial derivative taken. With increasing noise variance, the exponential terms diminish due to the noise variance factor in the exponent. The multiplicative factor in powers of $1/\sigma_\eta^2$ further decrease the higher-order terms to zero. Therefore, the first term of (10) approaches zero. The second term also approaches zero with similar observations for lower-order partial derivatives of A. Therefore, with high noise variance, the constant coefficients of the series tend to zero due to increasing powers of $1/\sigma_\eta^2$ present, raised to the order of the term. ■

With this theorem, the higher-order terms do not contribute significantly to the Gaussian approximation. Therefore, for high noise variance values (low SNRs), the LLR values can be approximated to be Gaussian.

For higher SNR values, the approximation loses its integrity with the higher contribution by higher-order terms of the expansion. As the simulation results will show, this approximation is accurate over the range of SNR that corresponds to the bit error probability of 10^{-3} to 10^{-4}. This is an important range in many practical applications.

II. LLR and BPSK Approximate Equivalence

Recall that a BPSK modulation scheme is composed of a one-dimensional signal constellation of two signal points. One point denotes a transmitted 0 and the other denotes a transmitted 1. For an AWGN channel, the mean of the received signal, r, can be either $\pm\sqrt{E_b}$, where E_b denotes the bit energy, depending on if 0 or 1 was transmitted. For equally likely signals, the decision threshold is 0.

The probability of error for this constellation can be easily shown to be [4]:

$$P_e = Q(\sqrt{\frac{2E_b}{N_0}}) = Q(\frac{\mu_r}{\sigma_r}). \tag{12}$$

Using this observation, and the Gaussian approximation of the LLR shown above, it can be argued that the process of deciding for bit m_k depending on the sign of $LLR(m_k)$ can be modeled by a BPSK system with signal points at $\pm\mu_{LLR}$ and noise variance of σ^2_{LLR}, where μ_{LLR} and σ^2_{LLR} denote the mean and the variance of the LLR as a Gaussian random variable, respectively. This means that the expression (12) can be used to compute the corresponding bit error probability. Using this model, the channel coding component (i.e., channel encoder, channel, and channel decoder) of a communications system can be replaced by a BPSK model, with mean equal to μ_{LLR} and noise variance equal to σ^2_{LLR}.

III. Analysis of Simulation Methods

An analysis of conventional simulation methods and the new approximation is now carried out to obtain the variance associated with calculating the probability of bit error by each method. These variances will then be compared, for a given probability of bit error, to illustrate the advantage of the approximation.

Conventional simulation methods call for the computer simulation of coded systems such that a preset number of errors occur to ensure that the precision of the resulting probability is not affected by statistical fluctuations. Suppose that a bit b_i is transmitted and $\hat{b}_i$ is decoded. Define the error event ϵ_i as,

$$\epsilon_i = \begin{cases} 1 & \text{when } b_i \neq \hat{b}_i \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the random variable E can be defined as

$$\mathrm{E} = \frac{1}{N}\sum_{i=1}^{N}\epsilon_i. \tag{13}$$

This random variable represents the probability of error, where N is the total number of bits transmitted, and its mean and variance can be shown to be

$$\begin{aligned}\bar{\mathrm{E}} &= \overline{\frac{1}{N}\sum_{i=1}^{N}\epsilon_i} \\ &= P_e \quad \text{(by definition)}\end{aligned} \tag{14}$$

$$\begin{aligned}\sigma^2_{\mathrm{E}} &= \frac{P_e}{N}(1-P_e) \\ &\approx \frac{P_e}{N} \;\; \text{when } P_e \text{ is small.}\end{aligned} \tag{15}$$

To compute the mean and the variance of the LLR, one can use either the expressions based on weight enumeration functions given earlier, or follow a simulation to gather samples of the LLR and use them to estimate the corresponding mean and variance. In the following, we concentrate on simulation methods for this purpose.

Analysis of the approximation method begins with a discussion of the estimators of the mean and variance, and then using these to obtain a probability density function for the ratio Z of the two quantities. The probability density function of Z can then be used to find the mean and variance of the $Q(Z)$.

The estimators for the mean and variance of the LLR used are maximum likelihood estimators (for Gaussian random variables). Considering that the N samples are i.i.d. Gaussian samples, with mean, μ, and variance, σ^2, the estimators considered are

$$\text{Mean } M,\ \overline{x} = \frac{1}{N}\sum_{i=0}^{N}x_i \tag{16}$$

$$\text{Variance } V^2,\ \sigma^2 = \frac{1}{N}\sum_{i=0}^{N}(x_i-\overline{x})^2 \tag{17}$$

where, M denotes the mean and V^2 denotes the variance. The mean and variance of each of the estimators are equal to,

$$\overline{M} = \mu \qquad Var(M) = \frac{\sigma^2}{N} \tag{18}$$

$$\overline{V^2} = \frac{N-1}{N}\sigma^2 \qquad Var(V^2) = \frac{2(N-1)}{N^2}\sigma^4\,. \tag{19}$$

Note that the estimator for the variance in (19) is biased. We will later show that the corresponding estimate of the ratio becomes asymptotically unbiased. It can be also shown that the two estimators are uncorrelated. For a large number of samples N, the two random variables, M and V^2, are Gaussian distributed. Since the two are uncorrelated and Gaussian, the the two estimators are independent [1, 5]. Using this fact, the probability density function of the ratio $Z = \frac{M}{V}$ can be found. The numerator is shown to be a Gaussian random variable, $\sim N(\frac{\mu\sqrt{N}}{\sigma}, 1)$, and the denominator is found to be a Chi-distributed random variable with N degrees of freedom and $\sigma^2 = 1$. The corresponding probability density function of the ratio is given by

$$f_Z(z) = \frac{\exp\{-\frac{\gamma^2}{2(z^2+1)}\}}{2^{\frac{N-2}{2}}\,\Gamma\left(\frac{N}{2}\right)} \frac{1}{\sqrt{z^2+1}^{\,N+1}} \cdot \left[\sum_{k=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{2k} \left(\frac{\gamma z}{\sqrt{z^2+1}}\right)^{N-2k} \frac{(2k)!}{k!2^k}\right] \tag{20}$$

where, $\gamma = \frac{\mu\sqrt{N}}{\sigma}$.

The r^{th} moment of Z is found to be

$$E[Z^r] = \left(\frac{1}{2}\right)^{\frac{r}{2}} \frac{\Gamma\left(\frac{1}{2}(N-r)\right)}{\Gamma\left(\frac{N}{2}\right)} \sum_{k=0}^{\lfloor \frac{r}{2} \rfloor} \binom{r}{2k} \left(\frac{\mu\sqrt{N}}{\sigma}\right)^{r-2k} \frac{(2k)!}{2^k k!}. \tag{21}$$

This is used to formulate the mean and variance of the Q-function. The estimator of the r^{th} moment is asymptotically unbiased, requiring no further modification to obtain true values.

The Q-function is expressible by a series expansion as,

$$Q(Z) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \left[\sum_{k=0}^{\infty} (-1)^k \frac{Z^{2k+1}}{k!\,(2k+1)\cdot 2^k}\right] \tag{22}$$

Using the r^{th} moments of Z from (21), and (22) from above, the mean and variance of Q(Z) is found to be

$$\begin{aligned} E[Q(z)] =& \overline{Q(z)} \\ =& \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \sum_{k=0}^{\infty} (-1)^k \left(\frac{1}{2}\right)^{\frac{2k+1}{2}} \frac{\Gamma\left(\frac{1}{2}(N-2k-1)\right)}{\Gamma\left(\frac{N}{2}\right) k!\,(2k+1)\cdot 2^k} \cdot \\ & \sum_{i=0}^{\lfloor \frac{2k+1}{2} \rfloor} \binom{2k+1}{2i} \left(\frac{\mu\sqrt{N}}{\sigma}\right)^{2k+1-2i} \frac{(2i)!}{2^i\, i!} \end{aligned} \tag{23}$$

$$\begin{aligned} \sigma^2_{Q(Z)} =& E[Q(z)^2] - E[Q(z)]^2 \\ =& \frac{1}{2} + \overline{Q(z)} + \frac{1}{\sqrt{2\pi}} \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{(-1)^{i+j}}{i!\,j!\,(2i+1)(2j+1)\cdot 2^{i+j}} \cdot \\ & \left(\frac{1}{2}\right)^{i+j+1} \frac{\Gamma\left(\frac{1}{2}(N-2(i+j)-2)\right)}{\Gamma\left(\frac{N}{2}\right)} \cdot \\ & \sum_{m=0}^{i+j+1} \binom{2(i+j)+2}{2m} \left(\frac{\mu\sqrt{N}}{\sigma}\right)^{2(i+j)+2-2m} \frac{(2m)!}{m!\,2^m} \\ & - \overline{Q(z)}^2, \end{aligned} \tag{24}$$

respectively.

IV. Numerical Results

Comparing the variances in expressions (15) and (24), for different N, tables I and II are obtained.

The fifth column of the table presents the ratio of the variances. It can be seen that variance of the approximation method is always smaller for a given probability of bit error. This translates into the approximation method being more precise than conventional methods, and therefore, the number of samples needed can be reduced. For example, referring to tables I and II, for a $\frac{\mu}{\sigma}$ value of 3, using conventional methods, the variance of 1.35e-8 is obtained with 100000 samples, while an even smaller variance (1.08e-8) can be obtained with 10000 samples using the proposed model. This is a factor of 10 reduction in the number of samples needed to obtain similar precision in the results.

Finally, soft-output decoding simulation results are presented for two binary linear codes: (8,4,4) Reed Muller code; and (24,12,8) Golay code.

Figure 1 presents the simulation results of the Reed Muller code over an AWGN channel. The solid line represents the conventionally simulated bit error probability curve while the dotted line represents the approximation model presented in this paper.

$\frac{\mu}{\sigma}$	P_e	σ^2_{E}	$\sigma^2_{Q(Z)}$	Ratio $\frac{\sigma^2_{\mathrm{E}}}{\sigma^2_{Q(Z)}}$
1	1.5866e-1	1.5866e-5	8.78160e-6	1.81
2	2.2750e-2	2.2750e-6	8.746385e-7	2.60
3	1.3499e-3	1.3499e-7	1.0841e-8	12.45
4	3.1671e-5	3.1671e-9	1.6355e-11	193.6

TABLE I
Comparison of Variances, $N = 10000$

$\frac{\mu}{\sigma}$	P_e	σ^2_{E}	$\sigma^2_{Q(Z)}$	Ratio $\frac{\sigma^2_{\mathrm{E}}}{\sigma^2_{Q(Z)}}$
1	1.5866e-1	1.5866e-6	8.7823e-7	1.81
2	2.2750e-2	2.2750e-7	8.7452e-8	2.60
3	1.3499e-3	1.3499e-8	1.0807e-9	12.49
4	3.1671e-5	3.1671e-10	1.6143e-12	196.2
5	2.8665e-7	2.8665e-12	2.9958e-16	9568.5

TABLE II
Comparison of Variances, $N = 100000$

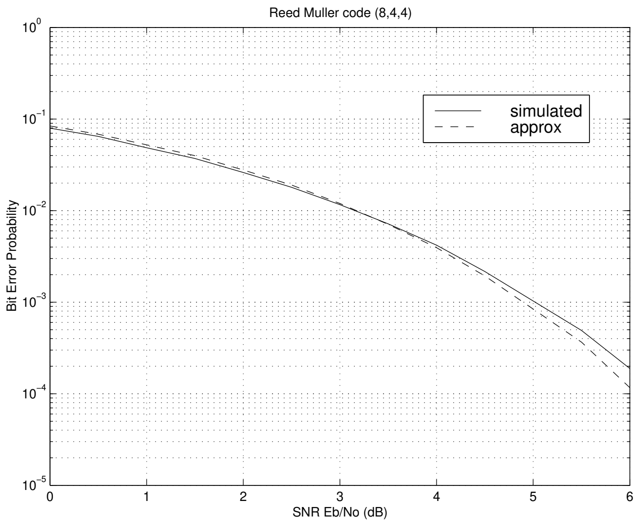

Fig. 1. Bit Error Performance Comparison for the Reed Muller code

It is observed that the dotted line closely follows the solid simulation curve, more so for lower SNR values. For high SNR (i.e., low noise variance), the higher order terms become more significant, and therefore cannot be neglected. Similar observations can be made for the Golay code, for which the simulation results over an AWGN channel are depicted in figure 2.

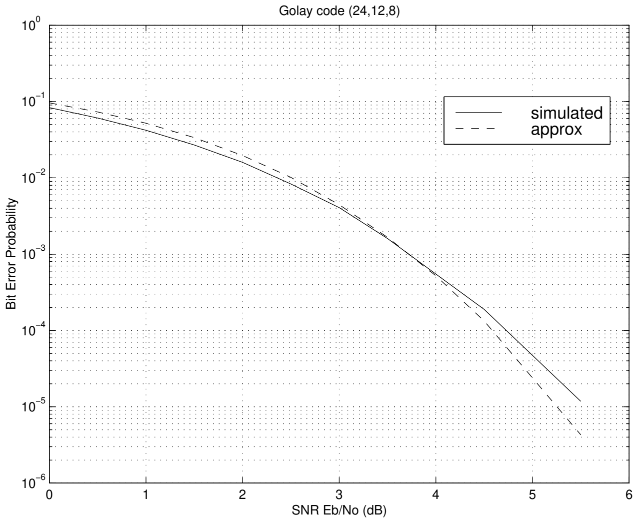

Fig. 2. Bit Error Performance Comparison for the Golay code

Chao *et al.* [6] evaluated the performance of binary block codes at low SNR values using a series expansion for the probability of correct decoding and considering only the first two terms of the series (zeroth and first-order). They give numerical results for the performance of a biorthogonal code with 16 codewords. It can be shown through a rotation of coordinates that this code is equivalent to the $(8,4,4)$ Reed-Muller code considered in this paper. Therefore, the results of figure 1 of [6, pp. 1686] can be directly compared with the results shown graphically in figure 3. The results of the approximation described in this paper are more precise over a wider range of SNR values. Similar first-order results can be shown for the Golay code in figure 4.

V. Conclusions

The bit error performance of a binary linear code can be approximated by approximating the LLR as being Gaussian distributed. Numerical results are presented which show that the proposed model provides a good approximation, especially for lower SNR values. The approximation requires fewer samples to obtain the same precision in the probability of error, and this translates into a time-savings for simulations. The proposed model allows us to replace a complex channel coding scheme by a simple BPSK model, with signal points at $\pm\mu_{LLR}$ and noise power σ^2_{LLR}.

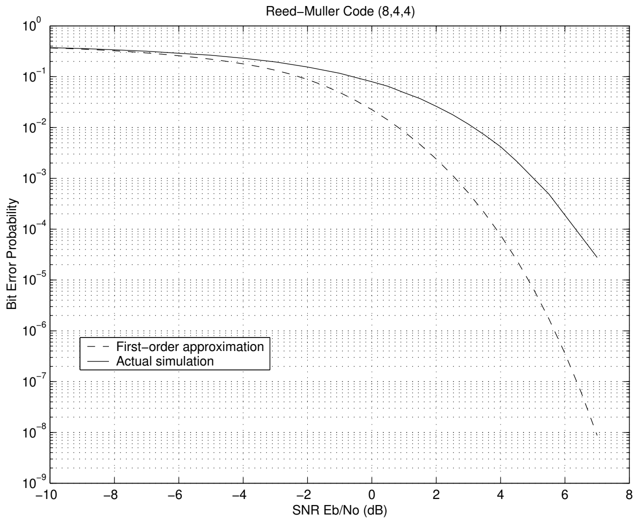

Fig. 3. First-Order Approx. for the Bit Error Performance of the $(8,4,4)$ Reed-Muller code

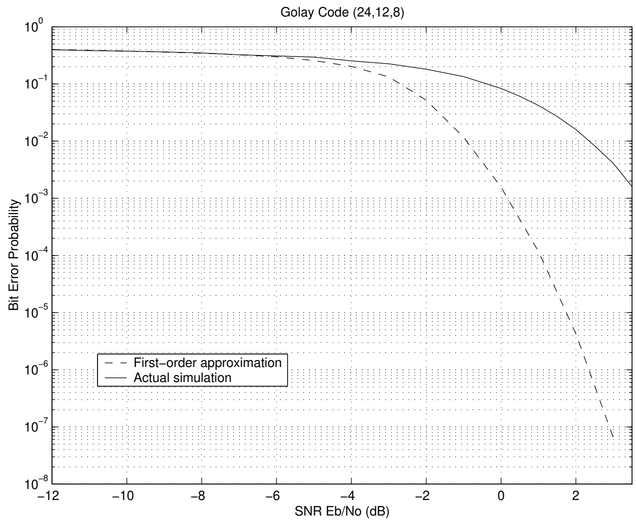

Fig. 4. First-Order Approx. for the Bit Error Performance for the $(24,12,8)$ Golay code

References

[1] P. Chaudhari, "Analytical Methods for the Performance Evaluation of Binary Linear Block Codes," M.A.Sc. thesis, Dept. of Elec. and Comp. Eng., University of Waterloo, Ontario, Canada, Spring 2000.

[2] P. Chaudhari and A. K. Khandani, "Statistical Analysis of the Soft-Output Decoding of Binary Linear Block Codes," Tech. Rep., University of Waterloo, Waterloo, Ontario, Canada, May 2000, E&CE#2000-05.

[3] D. Zwillinger, Ed., *Standard Mathematical Tables and Formulae*, CRC Press, Boca Raton, 30th edition, 1996.

[4] J. G. Proakis, *Digital Communications*, McGraw-Hill, New York, 3rd edition, 1995.

[5] Harald Cramér, *Mathematical Methods of Statistics*, Princeton University Press, Princeton, 1999.

[6] C.-C. Chao, R. J. McEliece, L. Swanson, and E. R. Rodemich, "Performance of Binary Block Codes at Low Signal-to-Noise Ratios," *IEEE Trans. Inform. Theory*, vol. 38, no. 6, pp. 1677–1687, Nov. 1992.