Bit Error Probability for Maximum Likelihood Decoding of Linear Block Codes

Marc P.C. Fossorier 1, Shu Lin 1 and Dojun Rhee 2

1 Dept. of Electrical Engineering University of Hawaii at Manoa Honolulu, HI 96822, USA
2 LSI LOGIC Corporation, 1525 McCarty Blvd, MS G-815, Milpitas, CA 95035, USA
Email: marc@siliki.eng.hawaii.edu

Abstract — In this paper, the bit error probability \( P_b \) for maximum likelihood decoding of binary linear codes is investigated. The contribution of each information bit to \( P_b \) is considered. For randomly generated codes, it is shown that the conventional approximation at high SNR \( P_b \approx (d_H/N) \cdot P_e \), where \( P_e \) represents the block error probability, holds for systematic encoding only. Also systematic encoding provides the minimum \( P_b \) when the inverse mapping corresponding to the generator matrix of the code is used to retrieve the information sequence. The bit error performances corresponding to other generator matrix forms are also evaluated. Although derived for codes with a generator matrix randomly generated, these results are shown to provide good approximations for codes used in practice. Finally, for decoding methods which require a generator matrix with a particular structure such as trellis decoding or algebraic-based soft decision decoding, equivalent schemes that reduce the bit error probability are discussed.

I. INTRODUCTION

In this paper, we consider the minimization of the bit error probability \( P_b \) for maximum likelihood decoding (MLD) of linear block codes. Although not optimum, this minimization remains important as MLD has been widely used in practical applications. We assume that the information sequence of length \( K \) is recovered from the decoded codeword based on the inverse mapping defined from the generator matrix of the code. For block codes, the large error coefficients can justify this strategy which is explicitly or implicitly used in many decoding methods such as conventional trellis decoding, multi-stage decoding or majority-logic-decoding. Therefore, for a particular code and the same optimal block error probability, we determine the best encoding method for delivering as few erroneous information bits as possible whenever a block is in error at the decoder output. We first derive a general upper bound on \( P_b \) which applies to any generator matrix and is tight at medium to high signal to noise ratio (SNR). This bound considers the individual contribution of each information bit separately. For randomly generated codes, we then show that the systematic generator matrix (SGM) provides the minimum bit error probability. To this end, a submatrix of the generator matrix defining an equivalent code for the bit considered is introduced. Note that a similar general result holds for the optimum bit error probability related to the BSC [2]. We finally discuss how to achieve this performance whenever the systematic encoding is not the natural choice, as for trellis decoding [3] or for MLD in conjunction with algebraic decoding [4]-[8]. For example, for trellis decoding of the \((32,26,4)\) Reed-Muller (RM) code, at low SNR a performance degradation of more than 1 dB is recovered with the proposed method. Minimizing the bit error probability associated with MLD becomes even more important whenever the considered block code is used as the inner code of a concatenated coding system [9].

II. BIT ERROR PROBABILITY FOR MLD

Suppose an \((N, K, d_H)\) binary linear code \( C \) with generator matrix \( G \) is used for error control over the AWGN channel. Defining

\[
P_b = \frac{1}{K} \sum_{j=1}^{K} P_b(j),
\]

where \( P_b(j) \) represents the error probability for the \( j \)th bit in a block of \( K \) information bits delivered by the decoder, we obtain from the union bound

\[
P_b(j) \leq \sum_{i=d_H}^{N} \hat{w}_i(j) \hat{Q}(\sqrt{i}),
\]

where \( \hat{Q}(x) = (\pi N_0)^{-1/2} \int_{-\infty}^{\infty} e^{-n^2/N_0} dn \). We call \( \hat{w}_i(j) \) the effective error coefficient associated with the \( j \)th information bit with respect to the generator matrix \( G \).

We can prove the following theorem.

Theorem 1 Let \( w_i \) represent the number of codewords of weight \( i \) in the code \( C \) generated by \( G \) and let \( w_i(j) \) represent the number of codewords of weight \( i \) in the subcode generated by the matrix \( G(j) \) obtained after deleting row \( j \) in \( G \); then

\[
\hat{w}_i(j) = w_i - w_i(j).
\]

Theorem 1 depends on the mapping defined by \( G \) as it implicitly assumes that the inverse mapping corresponding to \( G \) is used to retrieve the information bits.
The weight distribution of RM codes is far from a bi-
value computed from (6) is the exact ratio, although
for various forms of generator matrices. In all cases, the
average bit error probability is expressed as

\[ P_b \leq \sum_{i=d_H}^{N} \left( \frac{1}{K} \sum_{j=1}^{K} \tilde{w}_i(j) \right) Q \left( \sqrt{i} \right), \tag{4} \]

For a code defined by a matrix \( G \) randomly generated, we
associate each information bit \( j \in [1, K] \) a matrix

\[ D_\alpha(j) = \begin{bmatrix} \bar{0} & \mathbf{I}_{\alpha-1} \\ \mathbf{I}_{\alpha-1} & 1 \end{bmatrix} \tag{5} \]

where \( \mathbf{I} \) and \( \mathbf{I}_{\alpha-1} \) represent the all-1 vector and the
identity matrix of dimension \( \alpha - 1 \) respectively. The
matrix \( D_\alpha(j) \) is defined as the dependency matrix
associated with dimension \( j \) of the generator
matrix \( G \). This matrix allows to derive the following
theorem.

**Theorem 2** Let consider an \( (N, K) \) linear block code
\( C \) with a generator matrix generated randomly. Then
the value \( \tilde{w}_i(j) \) corresponding to the dimension \( j \) with
dependency matrix \( D_\alpha(j) \) is well approximated by

\[ \tilde{w}_i(j) \approx 2^{-(N-K)} \sum_{i=0}^{\alpha \leq 1} \left( \frac{\alpha}{2l+1} \right) \left( \frac{N-\alpha}{i-(2l+1)} \right) \tag{6} \]

Theorem 2 indicates that the larger \( \alpha \), the larger the
corresponding \( P_b(j) \). Consequently, \( \alpha = 1 \) gives the
smallest bit error probability. For this case, \( D_1 = [1] \)
which corresponds to a systematic encoding. Therefore,
the optimum bit error probability for MLD at
medium to high SNR is achieved by a systematic encoding if the inverse-mapping defined by \( G \) is used to
retrieve the information bits. This strategy is intuitively
correct since whenever a code sequence estimated by the decoder is in error, the best strategy
to recover the information bits is simply to determine them independently. Otherwise, errors propagate. For \( \alpha = 1 \), (6) becomes [1]

\[ \tilde{w}_i(j) \approx 2^{-(N-K)} \binom{N-1}{i-1} \approx (i/N) w_i. \tag{7} \]

In that case only, at high SNR, the bit error probability
for MLD follows

\[ P_b \approx \left( \frac{d_H}{N} \right) w_{d_N} Q \left( \sqrt{d_H} \right). \tag{8} \]

For Reed-Muller (RM) codes of length \( N \leq 64 \), we
computed the ratios \( \tilde{w}_{d_N}(j)/w_{d_N} \) corresponding to (6)
for various forms of generator matrices. In all cases, the
value computed from (6) is the exact ratio, although
the weight distribution of RM codes is far from a bi-
nomial distribution.

### III. Applications

#### A. ML trellis decoding

ML trellis decoding is based on the trellis oriented generator matrix (TOGM) of the code considered [3]. If
this matrix is used for encoding, trellis decoding becomes suboptimum with respect to the bit error probability of MLD. We present a simple method to overcome this problem.

Let \( G_t \) denote the TOGM of the code \( C_t \). Then, by
row additions only, it is possible to obtain the generator
matrix \( G \) of an equivalent code \( C \) which contains
the \( K \) columns of the identity matrix. This matrix is
known as the reduced echelon form (REF). These operations modify the mapping between information bits and codewords, but since no column permutation has been realized, each codeword of \( C \) is still uniquely represented by a path in the trellis of \( C_t \). Therefore ML trellis decoding of the received sequence is still possible if we use \( G \) for encoding. The trellis decoder estimates the code sequence which is closest to the received sequence. Then the information bits are easily retrieved
due to the systematic nature of \( G \). Since no restrictions on \( G_t \) apply, the matrix \( G \) can be obtained for any possible trellis decomposition.

In [10], a specific ML trellis decoding algorithm for the
(63,57,3) Hamming code is proposed. The decoding is realized based on a generator matrix in cyclic form. It is also shown that an equivalent systematic representation outperforms the cyclic form by 0.4 dB at the BER \( 10^{-5} \). However, the decoding of the systematic code requires an additional step. By processing the generator matrix in cyclic form as described in this section, this additional step can be removed as the encoding matrix becomes \( G = [I_r; P_b] \). On the other hand, the cyclic structure no longer exits, but the encoder remains very simple.

Figures 1 and 2 depict the simulation results for the
(32,16,8) and (32,26,4) RM-codes respectively. For
both codes, we simulated ML decoding based on the
REF and the conventional TOGM described in [3], and
plotted the first term of the union bound derived from
(4). As expected from the results of Section II, we
observe a larger gap in error performance for the (32,26,4)
RM-code. At the bit error rate (BER) \( 10^{-6} \), the gap in performance for this code is about 0.2 dB, which is of the same order as the difference between closest cost decoding (CCD) and ML trellis decoding [11]. Also, we observe a much significant gap at high BER of 0.4 dB for the (32,16,8) code and 1.1 dB for the (32,26,4) code. This behavior becomes important if a concatenated coding scheme is used.

The extension of this method to multi-stage trellis decoding does not follow in a straightforward way. In general, multi-stage decoding methods exploit the decomposable structure of the code considered, so that row additions on the associated generator matrix can
destroy this structure. For example, CCD of $|u|u + v|$- 
component code exploits the repetition of the $u$- 
component code [11]. As a result, row additions in each 
component code generator matrix are allowed, but not 
from one matrix to the other. In addition, the propa-
gation of decoding errors between decoding stages also 
has to be considered when searching for the optimum 
encoding matrix associated with multi-stage decoding.

B. MLD in conjunction with algebraic decoding

Several soft decision decoding algorithms in conjunction 
with an algebraic decoder have been proposed [4]- [8]. In general, algebraic decoding is associated with a 
particular generator matrix form $G_a$. Therefore, if this 
form is used for encoding, the corresponding algorithm 
becomes suboptimum with respect to the bit error prob-
ability of MLD. Algebraic decoding algorithms can be 
divided into two classes, depending on whether the de-
coder delivers an estimate of the transmitted codeword 
of length $N$ or of the information sequence of length $K$. 
In the first case, the method of Section A extends 
in a straightforward fashion. Hence decoding of cyclic 
codes can be realized this way. However, a similar 
method is also possible for the second class of algebraic 
decoders. Again, this method is transparent with re-
spect to algebraic decoding, so that the conventional 
algebraic decoder corresponding to the code consid-
ered can still be used. This method simply consists of 
recording the row operations processed to obtain $G$ 
in REF form $G_a$ and applying the inverse operations 

to the information sequence delivered by the algebraic 
decoder.

Figure 3 depicts the improvement achieved by this 
method for Chase algorithm-2 with majority-logic-de-
coding for the (64,42,8) RM-code. The proposed 
method outperforms Chase algorithm-2 with conven-
tional majority-logic-decoding by 0.15 dB at the BER 
$10^{-5}$.

C. Concatenated coding

We consider the concatenated scheme presented in [12] 
where the inner code is a (64,40) subcode of the (64,42) 
RM code and the outer code is the NASA standard 
(255,223) RS code over $GF(2^8)$. The outer code is in-
terleaved to a depth of 5. For this scheme, Figure 4 
represents the simulated bit error performance for en-
coding with the TOGM and the REF. We observe that 
the systematic encoding outperforms the TOGM by 
about 0.2 dB at the BER $10^{-5}$. More importantly, we 
also notice that while the error performance curves cor-
responding to the inner codes differ by a constant value 
due to different error coefficients, the difference in bit 
error probability between the error performance curves 
corresponding to the concatenated system increases as 
the SNR increases.

IV. Conclusion

In this paper, we have shown that for many good 
codes, the SGM provides the best bit error probability 
for MLD when the inverse mapping of the generator 
matrix $G$ is used to retrieve the information se-
quence. Based on the presented results, we can con-
clude that a careful choice of the generator matrix be-
comes important when comparing different optimum, 
near-optimum or suboptimum soft decision decoding 
schemes. Generally, tenths of dB's separate the bit er-
or performance of such schemes, so that a poor choice 
of the generator matrix of one of the scheme may result 
in an important relative degradation.

By exploiting the fact that modifying the mapping 
between information bits and codewords is transpar-
ent to the decoder, we modified conventional trellis 
decoding and MLD in conjunction with an algebraic 
decoder so that these schemes achieve the same bit 
error performance as for systematic encoding. Hence 
the decoding becomes independent of the encoding and 
can simply be viewed as a process providing the most 
likely codeword of the codebook. As a result, the de-
coder structure remains the same as the conventional 
one but in some cases the decoded sequence requires 
an additional simple reprocessing.

References


---

Figure 1: Simulated and theoretical bit error probabilities for the (32,16,8) RM code with TOGM and REF.

Figure 2: Simulated and theoretical bit error probabilities for the (32,26,4) RM code with TOGM and REF.

Figure 3: Simulated bit error probabilities for Chase algorithm-2 of the (64,42,8) RM code with majority-logic-decoding in Boolean and systematic forms.

Figure 4: Simulated bit error probabilities for (255,223) RS outer code and (64,40,8) inner code, and encoding with REF and TOGM.