Simple Tight Performance Bound Based on the GFBT for Binary Linear Codes

Jia Liu¹, Mingyu Zhang¹, Rongjun Chen²*, Chaoyong Wang¹, Xiaofeng An¹ and Yufei Wang¹

¹School of Information Engineering, Jilin Engineering Normal University, 3050 Kaixuan Road, Kuancheng District, Changchun, China.
²School of Computer Science, Guangdong Polytechnic Normal University, 293 West Zhongshan Avenue, Tianhe District, Guangzhou, China.
*Email: crj321@163.com

Abstract. A simple tight upper bound, without any integral and optimal operations in its final version, is proposed over additive white Gaussian noise (AWGN) channels. We derive the simple bound both on the frame probability and on the bit error probability. The proposed bound is within the framework of Gallager's first bounding technique (GFBT), in which the Gallager region is chosen by the hamming distance, avoiding the limitation of the Euclidean distance. To compute the upper bound inside the Gallager region, we can tighten the union bound not only by collecting more information about the receiving vector which can cause the maximum-likelihood (ML) decoding error events, but also by employing the independence between the ML decoding error events and some positions of the received vectors. The proposed bound is tight since numerical results show that it is tighter than the proposed bound by Divsalar (without any integral and optimal operations) and the proposed bound by Polytyev (considered as one of the tightest upper bounds for the binary linear codes with lower rate).

1. Introduction

Error correcting codes play an important role on the high reliable transmission of the next generation mobile communication systems. It is very important to evaluate the maximum-likelihood (ML) decoding performance of an error correcting codes. It is difficult to describe its decoding error probability with an exact expression for a specific binary linear code. Recently, there are two methods to estimate the performance of error correcting codes, that is, Monte Carlo simulation and upper (lower) bounds. However, on the one hand, the time complexity of Monte Carlo simulation is very high under the condition of high signal-to-noise ratio (SNR). On the other hand, the result of Monte Carlo simulation is difficult to describe the relationship between the ML decoding error probability and system parameters of the code. Then, we pay more attention to the upper and lower bounding technology to estimate the performance of the code. The union bound is the simplest upper bound, but there are two disadvantages for the union bound. First, it is loose and even diverges (≥1) in the low-SNR region. Second, it requires the whole weight distribution, which may not be available for complicated codes. Most upper bounds, which are closer to the actual ML performance for a wider range of SNR, are constantly proposed, as noted by [1]. Many upper bounds are based on the 1961 Gallager-Fano bound, which is also called Gallager's first bounding technique (GFBT).

\[ \Pr\{E\} = \Pr\{E, y \in \mathcal{R}\} + \Pr\{E, y \notin \mathcal{R}\} \]
where \(E\) is defined as the error event, \(\bar{y}\) is defined as the received signal vector, and \(\mathcal{R}\) (the so-called good region) is defined as the Gallager region. As noted by Sason[1], the choice of Gallager region is very important for the upper bound technique and different upper bounds can be obtained by selecting different Gallager regions[2–7]. However, many upper bounds have more prohibitively computational complexity than the union bound. Exceptionally, Divsalar[3] proposed a simple tight upper bound (called the Divsalar bound) based on GFBT, without any integral and optimal operations in its final version. Recently, Ma et al.[4–5] derived union bounds using truncated weight spectrum based on GFBT in which the Gallager region is specified by a list decoding algorithm (called the Ma bounds in this paper). The Ma bounds[4–5] improve the union bound but have a similar complexity, only involving the \(Q\)-function.

In this paper, we derive the simple upper bound in a closed form over the AWGN channel, which does not need any integral form and has a lower computational complexity. This paper is organized as follows:

1. In Sec.2, the preliminaries are given.
2. In Sec.3, the proposed simple upper bounds on frame-error probability and bit-error probability are both based on GFBT, in which the Gallager region is chosen in the similar way as the recently proposed bound by Ma et al.[5]. The error probability inside the Gallager region can be upper-bounded by the union bound involving the truncated weight spectra of the code. This truncated union bound can be tighten by collecting more information about the receiving signal vector which can cause the error events and employing the independence between the error events and some positions of the received vectors.
3. In Sec.4, Numerical example is provided.
4. We conclude this paper in Sec.5.

2. Preliminaries

We denote \(\mathbb{F}_2 = \{0, 1\}\) and \(\mathcal{A}_2 = \{-1, +1\}\) to be the binary field and the bipolar signal set, respectively. For the binary linear block code \(C[n, k]\), when the sender sends the transmitted codeword \(c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}\), the binary phase shift keying (BPSK) is considered, that is

\[
\phi: \mathbb{F}_2^n \mapsto \mathcal{A}_2^n.
\]

After modulation, the vector transmitted in the channel is \(\underline{s} = \phi(\underline{c}) \in \mathcal{S}\), where \(s_t = 1 \pm 2c_t\), \(0 \leq t \leq n - 1\). We denote \(\mathcal{S}\) to be the set of signal vectors after all the code words are modulated. Assuming that the received signal vector is \(\underline{y}\). Because of the interference of noise and other factors in the channel, the received signal vector \(\underline{y}\) is often different from the transmitted signal vector \(\underline{s}\). In fact, the ML decoding criterion is equivalent to finding a signal vector \(\hat{s} \in \mathcal{S}\) to maximize the probability \(p(\underline{y} | \hat{s})\), so as to translate the received vector \(\underline{y}\) into \(\hat{s}\). If \(\hat{s} = \underline{s}\), the decoding is correct; otherwise, the decoding error occurs. ML decoding is the best decoding method, which can maximize the probability of correct decoding.

For AWGN channel, the signal vector \(\underline{s}\) is transmitted on the channel. We assume \(\underline{y} = \underline{s} + \underline{z}\) to be the received signal vector, where \(\underline{z}\) is a sample of Gaussian white noise process with mean value of 0 and variance of \(\sigma^2\). According to the ML decoding criterion, we should find a signal vector \(\hat{s} \in \mathcal{S}\) to maximize the probability \(p(\underline{y} | \hat{s})\). Considering that the channel is discrete and memoryless, then we have
\begin{equation}
p(y \mid \hat{s}) = \prod_{i=0}^{n-1} p(y_i \mid \hat{s}_i)
\end{equation}

\begin{equation}
= \prod_{i=0}^{n-1} \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(y_i - \hat{s}_i)^2}{2\sigma^2}}
\end{equation}

\begin{equation}
= \left( \frac{1}{\sqrt{2\pi\sigma}} \right)^n e^{-\frac{\sum_{i=0}^{n-1} (y_i - \hat{s}_i)^2}{2\sigma^2}}.
\end{equation}

It can be verified to make the maximum \( p(y \mid \hat{s}) \), the sum of accumulation \( \sum_{i=0}^{n-1} (y_i - \hat{s}_i)^2 \) is required to be the minimum. The Euclidean distance is defined by

\begin{equation}
\| y - \hat{s} \|^2 = \sum_{i=0}^{n-1} (y_i - \hat{s}_i)^2.
\end{equation}

For AWGN channel, the ML decoding criterion is equivalent to finding a signal vector to minimize the Euclidean distance of sum, which is also called the minimum Euclidean distance criterion. We focus on the AWGN channel in this paper. Because there is a one-to-one correspondence between \( \mathcal{C} \) and \( \mathcal{S} \), when we express a codeword, we do not distinguish between \( \mathcal{C} \) and \( \mathcal{S} \). We assume that the channel is binary input, output symmetric and memoryless, and that the binary linear block code is considered. Without loss of generality, we assume that the transmitted code word is all zero code word, because the error probability under ML decoding at this time does not depend on the specific code word to be transmitted, so the average decoding error probability is equal to the conditional error probability of all zero codeword \( \mathcal{C}^{(0)} \) to be transmitted.

The input output weight enumeration functions (IOWEF) of a binary linear block code \( C[n,k] \) are defined as:

\begin{equation}
A(X,Z) = \sum_{i,j} A_{i,j} X^i Z^j,
\end{equation}

in which \( X,Z \) are the two dummy variables \( X,Z \), \( A_{i,j} \) denotes the number of codewords whose Hamming weight is \( j \) when the Hamming weight of the input information bit is \( i \). The weight enumeration function (WEF) can be expressed as:

\begin{equation}
A(1,Z) = \sum_{j} A_j Z^j,
\end{equation}

in which

\begin{equation}
A_j = \sum_{i} A_{i,j} , \quad 0 \leq j \leq n .
\end{equation}

3. The Proposed Simple Upper Bound

In this section, the suboptimal list decoding algorithm (algorithm 1), proposed by Ma bounds [4-5], will be used to define the following optimal Gallager region in (13).

Algorithm 1: (A list decoding algorithm)

1. Firstly, we should make hard decisions of the received vector, i.e.,

\begin{equation}
\hat{y}_t = \begin{cases} 
0, & y_t > 0 \\
1, & y_t \leq 0
\end{cases}
\end{equation}
Then we have the memoryless binary symmetric channel (BSC) in which the cross probability is

\[ p_b = \mathcal{O}\left( \frac{1}{\sigma} \right) \]  

(12)

2. Secondly, we need list all codewords within the Hamming sphere with center at \( \hat{y} \) of radius \( d^* \geq 0 \). We denote the resulting list as \( \mathcal{L}_2 \).

3. Finally, if \( \mathcal{L}_2 \) is empty, we declare a decoding error; otherwise, we should find the codeword \( \hat{c}^* \in \mathcal{L}_2 \) which is closest to the received vector \( y \).

Then, the Gallager region \( R \) is defined by

\[ R = \{ y \mid \hat{c}^{(0)} \in \mathcal{L}_2 \} . \]  

(13)

Proposition 1:

\[ \Pr\{ E \} \leq \min_{0 \leq d' \leq n} \left\{ \sum_{d=2d'} \Pr\{ E_d, W_H(\hat{y}) \leq d^* \} + B(p_b, n, d^* + 1, n) \right\} , \]  

(14)

where

\[ B(p, N_t, N_i, N_u) = \sum_{m=N_t}^{N_i} \binom{N_t}{m} p^m (1-p)^{N_t-m} . \]  

(15)

Proof: See the detail proof in [5].

Therefore, for any given \( d \) and \( d^* \), we only need to calculate the upper bound of probability \( \Pr\{ E_d, W_H(\hat{y}) \leq d^* \} \). Different from the previous works by Ma et al [5], we notice that the Hamming weight of the “right” part (to be precisely specified below) of \( \hat{y} \) can not be greater than \( \left[ d^* - d/2 \right] \). We can use this fact to further reduce the possibility of repeated calculation of error probability of decoding, so as to improve the compactness of the upper bound technology. We assume that \( A_d \geq 1 \) and all codewords of weight \( d \) are represented as \( \zeta^{(\ell)} = (1, \cdots, \ell, \cdots, 0) \). Let \( E_{0 \leq \ell} \) be the event that \( \zeta^{(\ell)} \) is closer to \( y \) than \( \zeta^{(0)} \).

3.1. Simple Tight Upper Bound on the Frame-Error Probability

Lemma 1

\[ \Pr\{ E_d, W_H(\hat{y}) \leq d^* \} \leq \frac{A_d \cdot e^{2\sigma} \sigma}{\sqrt{2\pi d}} B(p_b, n - d, 0, \left| d^* - d/2 \right|) . \]  

(16)

Proof: We define \( \zeta^{(1)} = (1 \cdots 10 \cdots 0) \). Denote \( y_d^{d-1} = (y_0, \cdots, y_{d-1}) \) and \( y_d^{n-1} = (y_d, \cdots, y_{n-1}) \). Obviously, only \( y_d^{d-1} \) can generate the ML decoding error events \( E_{0 \leq \ell} \). Let \( W_H(\hat{y}_d^{d-1}) = i \) and
We have

\[ W_H(\hat{y}_d^{n-1}) = j, \]

we have

\[ \hat{y} = (1\cdots10\cdots01\cdots10\cdots0). \]  

(17)

We point that a necessary condition for the ML decoding error events event \( E_{0\to1} \) is that the codeword \( \hat{c}^{(1)} \) is in the list \( \mathcal{L}_2 \). Hence \( W_H(\hat{c}^{(1)} - \hat{y}) \leq d^* \). By calculation, we get \( d - i + j \leq d^* \). Also we point that, since \( W_H(\hat{y}) \leq d^* (y \in \mathcal{R}) \), we get \( i + j \leq d^* \). Then, we can verify that \( j \leq \left\lfloor d^* - \frac{d}{2} \right\rfloor \). Finally, we have

\[
\Pr \{ E_{0 \to 1}, W_H(\hat{y}) \leq d^* \} \leq \sum_{j \in [d^* - d/2]} \Pr \{ E_{0 \to 1}, W_H(\hat{y}_d^{n-1}) \leq d^* - j, W_H(\hat{y}_d^{n-1}) = j \} 
\]

(18)

\[
\leq \sum_{j \in [d^* - d/2]} \Pr \{ E_{0 \to 1}, W_H(\hat{y}_d^{n-1}) = j \} 
\]

(19)

\[
= \Pr \{ E_{0 \to 1} \} \sum_{j \in [d^* - d/2]} \Pr \{ W_H(\hat{y}_d^{n-1}) = j \} 
\]

(20)

\[
= \Pr \{ E_{0 \to 1} \} \sum_{j \in [d^* - d/2]} \left( n - d \right) p_j^d (1 - p_j)^{n-d-j} 
\]

(21)

\[
= Q(\sqrt{d/\sigma})B\left( p_b, n-d, 0, \left\lfloor d^* - \frac{d}{2} \right\rfloor \right) 
\]

(22)

\[
\leq \frac{e^{x^2/2}}{\sqrt{2\pi d}} B(p_b, n-d, 0, \left\lfloor d^* - \frac{d}{2} \right\rfloor) 
\]

(23)

where

\[
Q(x) \leq \frac{e^{x^2/2}}{\sqrt{2\pi x}}. 
\]

(24)

By the symmetry properties of the joint bound and error event, the following upper bound can be obtained

\[
\Pr \{ E_d, W_H(\hat{y}) \leq d^* \} = \Pr \left\{ \bigcup_{1 \leq i \leq A_d} E_{0 \to 1}, W_H(\hat{y}) \leq d^* \right\} 
\]

\[ \leq \sum_{1 \leq i \leq A_d} \Pr \{ E_{0 \to 1}^i, W_H(\hat{y}) \leq d^* \} 
\]

\[ = A_d \Pr \{ E_{0 \to 1}, W_H(\hat{y}) \leq d^* \} 
\]

\[ \leq A_d \sum_{j \in [d^* - d/2]} \left( n - d \right) p_j^d (1 - p_j)^{n-d-j} 
\]

\[ \leq A_d Q(\sqrt{d/\sigma})B\left( p_b, n-d, 0, \left\lfloor d^* - \frac{d}{2} \right\rfloor \right) 
\]

(25)
\begin{equation}
7 \leq A_d \cdot e^{\frac{-x^2}{2\sigma^2}} B(p_b, n - d, 0, \left\lfloor d^* - d/2 \right\rfloor) \tag{26}
\end{equation}

Theorem 1: The simple tight upper bound on the frame-error probability

\[ \Pr(E) \leq \min \{ \sum_{\substack{d \leq 2d^* \leq n \atop 0 \leq d \leq n}} A_d \cdot e^{\frac{-x^2}{2\sigma^2}} B(p_b, n - d, 0, \left\lfloor d^* - d/2 \right\rfloor) + B(p_b, n, d^* + 1, n) \}. \tag{27} \]

Proof: From Lemma 1 and Proposition 1, we then have (27), completing the proof.

3.2. Simple Tight Upper Bound on the Bit-Error Probability

Define

\[ \hat{i}_d \overset{\Delta}{=} \max \{ i \mid A_{i,d} > 0 \}, \]
\[ A'_d = \sum_{i \leq k} A_{i,d}. \tag{29} \]

Theorem 2: The simple tight upper bound on the bit-error probability

\[ \Pr(E) \leq \min \{ \sum_{\substack{d \leq 2d^* \leq n \atop 0 \leq d \leq n}} A'_d \cdot e^{\frac{-x^2}{2\sigma^2}} B(p_b, n - d, 0, \left\lfloor d^* - d/2 \right\rfloor) + B(p_b, n, d^* + 1, n) \}. \tag{30} \]

Proof: Assuming that the input signal of the transmitter is \( U \) and the output binary vector of the decoder at the receiver is \( \hat{U} \), the bit error probability of the decoder can be defined as [8, p. 9]

\[ P_b = \frac{1}{k} \sum_{0 \leq d \leq k-1} \Pr\{ \hat{u}_i \neq u_i \}. \tag{31} \]

When all zero codewords are assumed to be the transmitted codewords, we have the bit error probability as following

\[ P_b = \mathbb{E}\left\{ W_H(\hat{U}) \right\} / k \]
\[ \tag{32} \]

in which \( \mathbb{E} \) represents the mathematical expectation.

Suppose we execute algorithm 1 (the suboptimal list decoding algorithm). Without loss of generality, when algorithm 1 declares the decoding failure, we assume that \( \hat{U} \) is uniformly random distributed.

We have

\[ kP_b = \Pr\{ y \in \mathcal{R} \} \mathbb{E}\{ W_H(\hat{U}) \mid y \in \mathcal{R} \} + \Pr\{ y \notin \mathcal{R} \} \mathbb{E}\{ W_H(\hat{U}) \mid y \notin \mathcal{R} \} \]
\[ \leq \Pr\{ y \in \mathcal{R} \} \mathbb{E}\{ W_H(\hat{U}) \mid y \in \mathcal{R} \} + k \Pr\{ y \notin \mathcal{R} \} \]
\[ \leq \sum_{d \leq 2d^*} \Pr\{ y \in \mathcal{R}_d \} \mathbb{E}\{ W_H(\hat{U}) \mid y \in \mathcal{R}_d \} + kB(p_b, n, d^* + 1, n). \tag{33} \]

Then, we pay close attention to deriving the upper-bound \( \Pr\{ y \in R^{(d)}_d \} \mathbb{E}\{ W_H(\hat{U}) \mid y \in R^{(d)}_d \} \) for any given \( d \leq 2d^* \). We assume the following partition \( R_d = \bigcup_{\ell} R^{(\ell)}_d \), where \( y \in R^{(\ell)}_d \), if and only if the suboptimal list decoding algorithm outputs codewords \( 1 \leq \ell \leq A_d \). When the decoder outputs \( c^{(\ell)} \), we assume that the corresponding message (input of the encoder) is \( \underline{u}^{(\ell)} \). By the definition \( A'_d \), we have
\[
\begin{align*}
\Pr\{y \in R_d\} & \leq \sum_{1 \leq i \leq A_y} \Pr\{y \in R_d^{(i)}\} W_H (u^{(i)}) \\
& \leq \sum_{1 \leq i \leq A_y} \Pr\{E_{0\rightarrow d}, y \in R\} W_H (u^{(i)}) \\
& \leq k A'_y Q \left( \frac{\sqrt{d}}{\sigma} \right) B(p_b, n - d, 0, d^* - 1) \\
& \leq \frac{k A'_y e^{2\gamma\sigma}}{\sqrt{2\pi d}} B(p_b, n - d, 0, \left\lfloor d^* - \frac{d}{2} \right\rfloor). \tag{34}
\end{align*}
\]

Substituting (34) into (33) and minimizing over \(d^*\), we have

\[
k \cdot P_e \leq \min_{0 \leq d \leq n} \left\{ \sum_{d' = 0}^{d - 2d} k \cdot A'_y e^{2\gamma\sigma} \frac{e^{-d^*}}{\sqrt{2\pi d}} B(p_b, n - d, 0, \left\lfloor d^* - \frac{d}{2} \right\rfloor) + k \cdot B(p_b, n, d^* + 1, n) \right\} \tag{35}
\]

to complete the proof, we divide \(k\) on the both sides of (35).

4. Numerical Examples

Figure 1 shows the comparison of the upper bound of the ML decoding frame error probability of [100,95] random codes. The upper bound technologies involved in the comparison include the simple upper bound technology proposed in this paper and Divsalar bound[3], the Ma bound[5] and TSB[2]. Through the data analysis, we know that the simple upper bound proposed in this paper is tighter than the Divsalar bound, Ma bound and TSB. Therefore, the simple upper bound proposed in this paper not only has the advantages of simple calculation, but also has the characteristics of tightness. The plots in Figure 1 rely on the weight spectra of [100, 95] random codes which can be found in [9].

![Figure 1](image-url)

**Figure 1.** A comparison of the upper bounds on the frame error probability for ML decoding of [100, 95] random codes
5. Conclusions
In this paper, a simple upper bound technique for binary linear block codes is proposed. The upper bound technique not only has a closed-form, but also has the characteristics of tightness. It can be applied to the fast analysis the performance of the unknown whole weight spectrum error correcting codes. The numerical results show that this bound is tighter than the Divsalar bound, the Ma bound and the TSB.

6. Acknowledgments
This work was supported in part by the National Natural Science Foundation of China under Grant 61401525, in part by the Scientific Research Planning Project of Education Department of Jilin Province named Research on Performance Bounds for Error Correcting Code in the Next Generation Mobile Communication Systems, in part by the Science and Technology Planning Project of Jilin City named Research on Key Technologies of wireless wearable health monitoring equipment, in part by the Doctoral Initiated Research Foundation Project under Grant BSKJ201820, BSKJ201821, BSKJ201822, in part by the University-level Scientific Research Foundation Project under Grant XYB201809, in part by Project for Distinctive Innovation of Ordinary Universities of Guangdong Province under Grant 2018KTSCX120. and the PhD Start-up Fund of Natural Science Foundation of Guangdong Province under Grant 2016A030310335.

7. References
[1] I. Sason and S. Shamai, “Performance analysis of linear codes under maximum-likelihood decoding: A tutorial,” in Foundations and Trends in Communications and Information Theory. Delft, The Netherlands: NOW, July 2006, vol. 3, no. 1-2, pp. 1–225
[2] G. Poltyrev, “Bounds on the decoding error probability of binary linear codes via their spectra,” IEEE Transactions on Information Theory, vol. 40, pp. 1284–1292, July 1994
[3] D. Divsalar, “A simple tight bound on error probability of block codes with application to turbo codes,” TMO Progress Report 42–139, JPL, pp. 1–35, November 1999
[4] X. Ma, C. Li, and B. Bai, “Maximum likelihood decoding analysis of LT codes over AWGN channels,” in Proc. the 6th International Symposium on Turbo Codes and Iterative Information Processing, Brest, France, September 2010
[5] X. Ma, J. Liu, and B. Bai, “New techniques for upper-bounding the MLD performance of binary linear codes,” in Proc. 2011 IEEE Int. Symp. Inform. Theory, Saint-Petersburg, Russian Federation, August 2011
[6] X. Ma, J. Liu, Q. Zhuang, and B. Bai, “New geometrical spectra of linear codes with applications to performance analysis,” in Proc. 2013 IEEE Int. Symp. Information Theory Workshop, Seville, Spain, August 2013
[7] J. Liu, “The parameterized Gallagers first bounds based on conditional triplet-wise error probability,” Mathematics and Computer in Simulation, vol. 163, pp. 32–46, September 2019.
[8] W. Ryan and S. Lin, Channel Codes: Classical and Modern. Cambridge, England: Cambridge University Press, 2009
[9] M. Twitto, “Tightened upper bounds on the ML decoding error probability of binary linear block codes and applications,” Master’s thesis, Department of Electrical Engineering, Technion-Israel Institute of Technology, Haifa, Israel, April 2006.