An Efficient Algorithmic Lower Bound for the Error Rate of Linear Block Codes

Firouz Behnamfar, *Member, IEEE,* Fady Alajaji, *Senior Member, IEEE,* and Tamás Linder, *Senior Member, IEEE*

Abstract

We present an efficient algorithmic lower bound for the block error rate of linear binary block codes under soft maximum likelihood decoding over binary phase-shift keying modulated additive white Gaussian noise channels. We cast the problem of finding a lower bound on the probability of a union as an optimization problem which seeks to find the subset which maximizes a recent lower bound – due to Kuai, Alajaji, and Takahara – that we will refer to as the KAT bound. The improved bound, which is denoted by LB-s, is asymptotically tight (as the signal-to-noise ratio (SNR) grows to infinity) and depends only on the code's weight enumeration function for its calculation. The use of a subset of the codebook to evaluate the LB-s lower bound not only significantly reduces computational complexity, but also tightens the bound specially at low SNRs. Numerical results for binary block codes indicate that at high SNRs, the LB-s bound is tighter than other recent lower bounds in the literature, which comprise the lower bound due to Séguin, the KAT bound (evaluated on the entire codebook), and the dot-product and norm bounds due to Cohen and Merhav.

Index Terms

Channel coding, linear block codes, weight spectrum of codes, probability of error, binary phase-shift keying, additive white Gaussian noise, lower bound, maximum likelihood decoding.

IEEE Transactions on Communications: submitted July 2005; revised February 2006. This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada and the Premier's Research Excellence Award (PREA) of Ontario.

The authors are with the Department of Mathematics and Statistics and the Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario K7L 3N6, Canada. T. Linder is also associated with the Computer and Automation Research Institute of the Hungarian Academy of Sciences.

E-mail: {firouz, fady, linder}@mast.queensu.ca, Phone: (613) 533-2398, Fax: (613) 533-2964.

I. INTRODUCTION

We study lower bounds for the codeword error probability of linear block codes for the binary phase-shift keying (BPSK) modulation and the additive white Gaussian noise (AWGN) channel under soft maximum-likelihood (ML) decoding. Let $A_1, A_2, ..., A_N$ be a finite number of events with positive probability in a probability space. de Caen's lower bound on the probability of the union of these events is given by [4]

$$P\left(\bigcup_{i=1}^{N} A_i\right) \geq \sum_i \frac{P(A_i)^2}{\sum_j P(A_i \cap A_j)}. \tag{1}$$

An application of de Caen's inequality is the evaluation of a lower bound on the codeword error probability (or error rate) of block codes. For a codebook $\mathcal{C} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, ..., \boldsymbol{c}_{M-1}\}$ of size M, the codeword error probability can be written as

$$P(\mathcal{E}) = \sum_{u=0}^{M-1} P\left(\mathcal{E}|\boldsymbol{s}_u\right) p(\boldsymbol{s}_u) = \sum_{u=0}^{M-1} P\left(\bigcup_{i\in\mathcal{S}} \epsilon_{ui} \middle| \boldsymbol{s}_u\right) p(\boldsymbol{s}_u), \tag{2}$$

where $\mathcal{E}$ is the codeword error event, $\boldsymbol{s}_u$ is the (modulated) signal corresponding to codeword $\boldsymbol{c}_u$, $P(\mathcal{E}|\boldsymbol{s}_u)$ is the conditional probability of error given that $\boldsymbol{s}_u$ is transmitted, $\mathcal{S} \triangleq \{0, 1, ..., M-1\}$ is the index set of the codewords, and ϵ_{ui} is the event that between codewords $\boldsymbol{s}_i$ and $\boldsymbol{s}_u$, $\boldsymbol{s}_i$ is decoded at the receiver. The computational complexity of evaluating the error rate via (2) is prohibitive even for moderate codebook sizes. For linear block codes under soft maximum likelihood decoding and for output-symmetric channels [10], equation (2) can be simplified to

$$P(\mathcal{E}) = P(\mathcal{E}|\boldsymbol{s}_u), \qquad u = 0, ..., M-1, \tag{3}$$

which significantly reduces the amount of calculations. In particular, for additive white Gaussian noise channels and BPSK signaling, using (1) with $u = 0$ results in

$$P(\mathcal{E}) = P(\mathcal{E}|\boldsymbol{s}_0) \geq \sum_{i=1}^{M-1} \frac{Q^2(\sqrt{2\Delta w_i})}{\sum_{j=1}^{M-1} \Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j})}, \tag{4}$$

where $\boldsymbol{s}_0$ is the modulated version of $\boldsymbol{c}_0$ which we assume to be the all-0 codeword, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-x^2/2} dx$ is the Gaussian tail function,

$$\Psi(\rho, x, y) = \frac{1}{2\pi\sqrt{1-\rho^2}} \int_x^\infty \int_y^\infty \exp\left\{-\frac{x^2 - 2\rho xy + y^2}{2(1-\rho^2)}\right\} dxdy$$

is the bivariate Gaussian function, $\Delta = E_b/N_0 r_c$ (with E_b being the average encoding power per uncoded bit, $N_0/2$ being the variance of the AWGN, and r_c being the channel code rate), $w_i \triangleq w(\boldsymbol{c}_i)$ is the Hamming weight of codeword $\boldsymbol{c}_i$, and,

$$\rho_{ij} = \frac{w(\boldsymbol{c}_i \boldsymbol{c}_j)}{\sqrt{w(\boldsymbol{c}_i) w(\boldsymbol{c}_j)}}. \tag{5}$$

We note that the upper limit in the sums in (4) still makes this bound too complex for most applications. Also, this bound requires the knowledge of not only the codeword weights (which are already known and tabulated), but also the weight of the product (logic AND) of codeword pairs. In an effort to resolve these problems, Séguin derived

in [9] a lower bound for (4) and hence a lower bound on the probability of error. Séguin's bound relies on the fact that $\Psi(\rho,\cdot,\cdot)$ is increasing in ρ and on the following upper bound on ρ_{ij}

$$\rho_{ij} \leq \kappa_{w_i w_j} \stackrel{\triangle}{=} \min\left\{\sqrt{\frac{w_i}{w_j}}, \sqrt{\frac{w_j}{w_i}}, \frac{w_i + w_j - D_{\min}}{2\sqrt{w_i w_j}}\right\}, \tag{6}$$

where $D_{\min}$ is the minimum distance of the code. Applying (6) to (4) results in Séguin's bound which is given by

$$P(\mathcal{E}|\boldsymbol{s}_0) \geq L_2 \stackrel{\triangle}{=} \sum_{s=1}^{n}\left(\frac{A_s Q^2(\sqrt{2\Delta s})}{Q(\sqrt{2\Delta s}) + (A_s - 1)\Psi(1 - \frac{D_{\min}}{2s}, \sqrt{2\Delta s}, \sqrt{2\Delta s}) + \sum_{t\neq 0,s} A_t \Psi(\kappa_{st}, \sqrt{2\Delta s}, \sqrt{2\Delta t})}\right), \tag{7}$$

where A_s is the number of codewords with weight s and n is the code blocklength.

The significance of Séguin's bound, which we will refer to as the L_2 lower bound, is three-fold. First, the L_2 bound depends only on the code's weight enumeration function. Second, Séguin proves in [9] that it approaches the union upper bound as the signal-to-noise ratio (SNR) grows to infinity,[1] making it asymptotically tight. Third, the upper limit in the sums in L_2 is given by the blocklength; hence, this bound is significantly more efficient to calculate than (4). The drawback of the L_2 bound is that it is loose at low SNRs.

de Caen's lower bound is tightened in [6], where the KAT bound is introduced. When used in the context of error analysis of block codes, the KAT lower bound is given by

$$\begin{aligned} P(\mathcal{E}|\boldsymbol{s}_0) \quad \geq \quad \text{KAT}(\mathcal{C}) \stackrel{\triangle}{=} \sum_{i\in\mathcal{C}, i\neq 0}\Bigg(&\frac{\theta_i Q^2(\sqrt{2\Delta w_i})}{\sum_{j\neq 0}\Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}) + (1-\theta_i)Q(\sqrt{2\Delta w_i})} \\ &+ \frac{(1-\theta_i)Q^2(\sqrt{2\Delta w_i})}{\sum_{j\neq 0}\Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}) - \theta_i Q(\sqrt{2\Delta w_i})}\Bigg), \end{aligned} \tag{8}$$

where

$$\theta_i = \frac{\beta_i}{\alpha_i} - \left\lfloor \frac{\beta_i}{\alpha_i} \right\rfloor,$$

with $\lfloor x \rfloor$ being the largest integer smaller than x, $\alpha_i = Q(\sqrt{2\Delta w_i})$ and

$$\beta_i = \sum_{j:j\neq i} \Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}).$$

Note that the above bound reduces to de Caen's lower bound if we set $\theta_i = 0$ for all i. The KAT bound is shown to be tighter than de Caen's bound in [6]. In [3], Dembo provides an alternative proof for the KAT bound and shows that it can improve over de Caen's bound by a factor of at most 9/8 (when both bounds operate on the same set of events).

Another lower bound on the probability of a union is derived in [2], which also includes the lower bound of de Caen as a special case. Based on this new inequality, two lower bounds on the error probability of block codes

[1] In this paper, by SNR we mean E_b/N_0.

are obtained in [2], which are referred to as the dot-product and norm bounds. Following the approach of Séguin, the dot-product and norm bounds can be evaluated using only the weight enumeration function of the code. The dot-product bound is calculated using the sub-collection of the minimum-weight codewords and is tighter at low SNRs. The norm bound requires the whole weight spectrum and is tighter at high SNRs. These bounds are shown through numerical results to be tighter than the L_2 bound [2].

In Section II we prove that the expression in (8) is still a lower bound when it is computed using the upper bound on ρ (as given in (6)) and when it is evaluated using a subset of the codebook. We will then present an algorithm to tighten the modified KAT bound. Numerical results are given in Section III and conclusions are drawn in Section IV.

II. An Algorithmic KAT Lower Bound

A. Use of a Subset

In order to find a lower bound on the probability of the union of a finite number of events $\{A_i, i \in \mathcal{J}\}$ (where $\mathcal{J} = \{1, 2, ..., N\}$), many methods (e.g., see [5]) are expressed as a maximization of a lower bound with respect to a sub-collection of these events. In fact, algorithms such as the one in [7] are stepwise search methods which are sensitive to the initialization, so their final sub-collection depends on the sets from which the search begins.

We note that the number of terms in the sums in (8) is $M - 1$ (where M is the codebook size); this leads to a high computational load even for codes of moderate size such as the BCH (63, 24) code [8]. One way to address this problem is to use the well known fact that

$$P\left(\bigcup_{i\in\mathcal{J}} A_i\right) \geq P\left(\bigcup_{j\in\mathcal{T}\subseteq\mathcal{J}} A_j\right).$$

Therefore, evaluation of (8) using only a sub-collection of the codebook will result in a valid lower bound for the error rate of codes, i.e.,

$$P(\mathcal{E}|\boldsymbol{s}_0) = P\left(\bigcup_{i\in\mathcal{S}} \epsilon_{0i} \,\middle|\, \boldsymbol{s}_0\right) \geq \text{KAT}(\mathcal{I} \subseteq \mathcal{C}), \tag{9}$$

where $\mathcal{I}$ is a subset of the codebook $\mathcal{C}$. The optimal subset (whose size and components depend on the SNR) is

$$\mathcal{I}^* = \arg\max_{\mathcal{I}\subseteq\mathcal{C}} \text{KAT}(\mathcal{I});$$

however, in general it is infeasible to determine. Our objective becomes then to determine a "good" subset $\mathcal{I}$ of $\mathcal{C}$ so that KAT($\mathcal{I} \subseteq \mathcal{C}$) in (9) is as large as possible. Also, to keep KAT($\mathcal{I} \subseteq \mathcal{C}$) with low complexity so that it can be computed using only the weight enumeration function of the code, we wish (as in [9] and [2]) to replace ρ_{ij} by κ_{w_i,w_j} as described in (6). However, (unlike [9] and [2]), it is no longer clear that such a replacement would result in a valid lower bound for $P(\mathcal{E}|\boldsymbol{s}_0)$ since $\Psi(\cdot,\cdot,\cdot)$ appears in both the numerator and denominator terms (in θ_i) of (8). This is ascertained in the following Lemma.

Lemma – Consider a linear block code $\mathcal{C}$. For a subset $\mathcal{I} \subseteq \mathcal{C}$, let $B_1(\mathcal{I}), B_2(\mathcal{I}), ..., B_n(\mathcal{I})$ be the weight enumerations of $\mathcal{I}$ (i.e., $B_i(\mathcal{I})$ is the number of codewords in $\mathcal{I}$ of weight i). Then the error rate of the code is lower bounded by

$$P(\mathcal{E}) = P(\mathcal{E}|\boldsymbol{s}_0) \geq \text{LB-s}(\mathcal{I}) \stackrel{\triangle}{=} \sum_{s=1}^{n} B_s(\mathcal{I}) Q^2(\sqrt{2\Delta s}) \left(\frac{\tilde{\theta}_s}{(2-\tilde{\theta}_s)Q(\sqrt{2\Delta s}) + S} + \frac{1-\tilde{\theta}_s}{(1-\tilde{\theta}_s)Q(\sqrt{2\Delta s}) + S} \right), \tag{10}$$

where

$$S = (B_s(\mathcal{I}) - 1)\Psi\left(1 - \frac{D_{\min}}{2s}, \sqrt{2\Delta s}, \sqrt{2\Delta s}\right) + \sum_{t \neq 0,s} B_t(\mathcal{I})\Psi(\kappa_{st}, \sqrt{2\Delta s}, \sqrt{2\Delta t}),$$

and

$$\tilde{\theta}_s = \frac{\tilde{\beta}_s}{\tilde{\alpha}_s} - \left\lfloor \frac{\tilde{\beta}_s}{\tilde{\alpha}_s} \right\rfloor,$$

with $\tilde{\alpha}_s = Q(\sqrt{2\Delta s})$ and

$$\tilde{\beta}_s = (B_s(\mathcal{I}) - 1)\Psi\left(1 - \frac{D_{\min}}{2s}, \sqrt{2\Delta s}, \sqrt{2\Delta s}\right) + \sum_{t \neq 0,s} B_t(\mathcal{I})\Psi(\kappa_{st}, \sqrt{2\Delta s}, \sqrt{2\Delta t}).$$

Proof – See Appendix.

Some points merit attention here. First, one should note in the above Lemma that $B_i(\mathcal{I})$ are not necessarily equal to $A_i(\mathcal{S})$ in (7). Second, using the approach of [3], one can verify that the ratio of the LB-s bound to the L_2 bound is still at most 9/8 when both bounds operate on the same set of codewords. Third, if, for a given subset $\mathcal{I}_1$, we have LB-s($\mathcal{I}_1$) > LB-s($\mathcal{C}$) (see the next subsection), then LB-s($\mathcal{I}_1$) is tighter than the original L_2 bound. As a result, LB-s($\mathcal{I}_1$) is asymptotically tight in the sense that it converges to the union upper bound as the SNR grows to infinity (because the L_2 bound is asymptotically tight).

B. Tightening the LB-s Bound

For each SNR, tightening the LB-s bound requires a suitable choice of the subset $\mathcal{I}$. We propose to do so by iteratively enlarging the sub-collection of codewords via the following algorithm:

1) Start from the initial set $\mathcal{I}_1$ of the minimum-weight codewords;
2) Add to $\mathcal{I}_1$ a codeword with the smallest weight possible to get $\mathcal{I}_2$;
3) If LB-s($\mathcal{I}_1$) > LB-s($\mathcal{I}_2$), stop;
4) Let $\mathcal{I}_1 = \mathcal{I}_2$ and go to step 2.

In the above algorithm, the search for the best subset stops in a very short time particularly at low SNRs where the minimum-weight codeword set is empirically observed to be optimal. The algorithm can provide significant improvements over the KAT bound evaluated using (6) particularly at low SNRs. For example, at SNR = 0 dB and

for the BCH (31, 16) code, the KAT bound equals 3.178×10^{-3} while the LB-s bound equals 3.831×10^{-2}, which is 12 times larger.[2]

The computational complexity of the LB-s bound is quite favorable compared with the dot-product and norm bounds of [2] which need to find other parameters via exhaustive search (see Section III). Nevertheless, as the code operates on larger data blocks (i.e., as k increases in $r_c = k/n$), computing the norm, dot-product, and even LB-s bounds tends to become infeasible. We therefore propose to replace the second step of the above algorithm with

2′) Add to $\mathcal{I}_1$ *all* codewords with the smallest weight possible to get $\mathcal{I}_2$;

Using the above step, one needs to run the algorithm for at most n times instead of $2^k - 1$ times. We have observed that the loss caused by the above step (as compared with the original algorithm) is negligible, but the run time is exponentially smaller.

III. Numerical Results and Discussion

We first compare the tightness of the LB-s bound versus the KAT bound which is evaluated using the upper bound on ρ_{ij} in (6) (so it is indeed equal to LB-s($\mathcal{C}$)) in Table I for the BCH (63, 10) code. Table I also demonstrates the gradual enlargement of the subset $\mathcal{I}_1$ with respect to the SNR. To show the behavior of the LB-s bound, the first version of the algorithm in Subsection II-B is used for this table. The weight spectrum of the code is specified by $(s, B_s(\mathcal{I})) \in \{(0,1), (27,196), (28,252), (31,63), (32,63), (35,252), (36,196), (63,1)\}$. The LB-s($\mathcal{I}_1$) bound is observed to be tighter than LB-s($\mathcal{C}$) particularly at low SNRs. As the SNR grows, the best codeword set $\mathcal{I}_1$ grows as well, reducing the gap between the two bounds. At SNR ≥ 8 dB, LB-s($\mathcal{I}_1$) uses the entire codebook except for the all-1 codeword (recall that we are computing the lower bounds on $P(\mathcal{E}|\boldsymbol{s}_0) = P(\mathcal{E})$, see (3)). Hence it converges to LB-s($\mathcal{C}$) as the SNR approaches infinity.

The second version of the algorithm in Subsection II-B is used to obtain the results in the rest of this section. Figure 1 compares the performance of the L_2, dot-product, norm, and LB-s bounds for the BCH (63, 24) code. At low SNRs (≤ 0 dB), the dot-product bound of [2] is the tightest bound among the above bounds. As the SNR grows, the norm and then the LB-s bounds become the tightest. This is indicated in more detail in Table II, where we have tabulated the values of the bounds for a higher SNR range.

We have repeated the algorithm of Subsection II-B for the L_2 bound to obtain a tighter version of this bound, referred to as the L_2-s bound. The results are reported in Table III (it can be easily verified that L_2-s is a valid lower bound). The L_2-s bound is seen to be significantly tighter than the L_2 bound especially at lower SNRs, but it

[2]In general, the LB-s bound seems to be looser than the dot-product bound of [2] at low SNRs. In particular, for the BCH (31, 16) code, the LB-s bound is 72% of the dot-product bound at 0 dB. However, as will be explained in the next section, the LB-s bound is tighter than the dot-product and norm bounds for higher SNRs. For the BCH (31, 16) code, the LB-s is the tightest bound for SNR > 6.5 dB or error rates of less than 10^{-6}.

is never tighter than the norm bound of [2] or the LB-s bound derived here. Table III also emphasizes the last point observed in Table II for the Golay (24, 12) code: for SNR $>$ 6 dB, the LB-s bound is tighter than the other bounds for the entire SNR range considered in the table. A similar behavior is observed for other linear block codes.

An important point to note is the computation time of the bounds. The second version of the algorithm to compute the LB-s bound in Subsection II-B drastically reduces the computation time for the LB-s bound. For example, as mentioned in Table II, the run time of the norm bound in the -5 to 10 dB range (with 1 dB increments) was 32076 seconds (i.e., more than 8.9 hours) on a SUN UltraSparc platform, while it was only 4 seconds for the LB-s bound (note that the dot-product bound is looser than the LB-s bound at high SNRs and also has a longer run-time). A similar behavior is observed in Table III. The run-time of the LB-s bound for other high-rate codes with large blocklengths, for which computing the norm bound becomes infeasible, is also in the same order. Reduced run time together with the fact that the LB-s bound is tight at high SNRs, are two main advantages of the LB-s bound.

IV. Conclusions

We derived a simple algorithmic lower bound on the error probability of soft ML decoded block codes based on the KAT lower bound. The bound, denoted by LB-s, is asymptotically tight and it can be calculated using only the weight enumeration information of the underlying code. It is observed that the LB-s lower bound is tighter than the original KAT lower bound everywhere and it is tighter than the other lower bounds considered in this paper at high SNRs. The computation time of the bound is also signifi cantly shorter than the bounds studied here. The results of this paper were presented for the AWGN channel. Nevertheless, they can be used for other channel models, such as block Rayleigh fading or space-time orthogonal block coded channels. The required pairwise error probability expressions for such channels can be found in [1].

Acknowledgment

The authors would like to thank Asaf Cohen for providing them with his source code to compute the dot-product and norm bounds.

Appendix

Here we prove that the LB-s bound is still a lower bound for $P\left(\mathcal{E}|\boldsymbol{s}_0\right)$. Similar to [3], we write (8) as

$$\sum_i Q\left(\sqrt{2\Delta w_i}\right) g(K_i, \theta_i), \tag{11}$$

where

$$g(K,\theta) = \frac{\theta}{K+1} + \frac{1-\theta}{K}$$

and K_i, which is a positive integer, and $\theta_i \in [0,1)$ are found from

$$\sum_j \Psi\left(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) = (K_i + \theta_i) Q\left(\sqrt{2\Delta w_i}\right). \tag{12}$$

We now want to prove that when $\Psi\left(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right)$ is replaced with its upper bound, (11) still gives a lower bound for $P(\mathcal{E}|\boldsymbol{s}_0)$. To this end, we first let

$$\sum_j \Psi\left(\kappa_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) = (\tilde{K}_i + \tilde{\theta}_i) Q\left(\sqrt{2\Delta w_i}\right), \tag{13}$$

where $\tilde{K}_i$ is a positive integer and $\tilde{\theta}_i \in [0,1)$, and show that

$$g(K_i, \theta_i) \geq g(\tilde{K}_i, \tilde{\theta}_i). \tag{14}$$

From $\Psi\left(\kappa_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) \geq \Psi\left(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right)$, (12), and (13), it follows that

$$\tilde{K}_i + \tilde{\theta}_i \geq K_i + \theta_i. \tag{15}$$

We now consider two cases: *i)* $\tilde{K}_i = K_i$ and *ii)* $\tilde{K}_i > K_i$.

Case i) $\tilde{K}_i = K_i$: In this case, it follows from (15) that $\tilde{\theta}_i \geq \theta_i$. Therefore,

$$g(\tilde{K}_i, \tilde{\theta}_i) = g(K_i, \tilde{\theta}_i) = \frac{\tilde{\theta}_i}{K_i + 1} + \frac{1 - \tilde{\theta}_i}{K_i} = \frac{1}{K_i} - \frac{\tilde{\theta}_i}{K_i(K_i+1)} \leq \frac{1}{K_i} - \frac{\theta_i}{K_i(K_i+1)} = g(K_i, \theta_i).$$

Therefore, (14) holds in the first case.

Case ii) $\tilde{K}_i > K_i$: For this case, we will show that $g(\tilde{K}_i, \tilde{\theta}_i) - g(K_i, \theta_i)$ is negative. We have

$$g(\tilde{K}_i, \tilde{\theta}_i) - g(K_i, \theta_i) = \frac{K_i(K_i+1)(\tilde{K}_i+1) - (K_i+1)\tilde{K}_i(\tilde{K}_i+1) + \theta_i\tilde{K}_i(\tilde{K}_i+1) - \tilde{\theta}_i K_i(K_i+1)}{K_i(K_i+1)\tilde{K}_i(\tilde{K}_i+1)}. \tag{16}$$

The denominator of (16) is clearly positive, so we need to consider its numerator which, after setting $\tilde{K}_i = K_i + n$ where $n \geq 1$ is an integer, reduces to

$$\underbrace{(\theta_i - \tilde{\theta}_i - n)}_{A} K_i^2 + \underbrace{((\theta_i - n^2) + 2n(\theta_i - 1) - \tilde{\theta}_i)}_{B} K + \underbrace{(n^2 + n)(\theta_i - 1)}_{C}.$$

In the above, both θ_i and $\tilde{\theta}_i$ are in $[0,1)$; therefore, $\theta_i - \tilde{\theta}_i < 1 \leq n$, hence $A < 0$. Also, $\theta_i < 1 \leq n$, hence $B < 0$ and $C < 0$. Because A, B, and C are all negative in the above (and K_i is positive), (14) also holds for the second case. This completes the proof of (14).

REFERENCES

[1] F. Behnamfar, F. Alajaji, and T. Linder, "Tight error bounds for space-time orthogonal block codes under slow Rayleigh flat fading," *IEEE Trans. Commun.*, pp. 952-956, June 2005.

[2] A. Cohen and N. Merhav, "Lower bounds on the error probability of block codes based on improvements on de Caen's inequality," *IEEE Trans. Inform. Theory*, vol. 50, pp. 290-310, Feb. 2004.

[3] A. Dembo, unpublished notes, communicated by I. Sason and A. Cohen, 2000.

[4] D. de Caen, "A lower bound on the probability of a union," *Discr. Math.*, vol. 169, pp. 217-220, 1997.

[5] E. G. Kounias, "Bounds on the probability of a union, with applications," *Ann. Math. Statist.*, vol. 39, no. 6, pp. 2154-2158, 1968.

[6] H. Kuai, F. Alajaji, and G. Takahara, "A lower bound on the probability of a finite union of events," *Discr. Math.*, vol. 215, pp. 147-158, Mar. 2000.

[7] H. Kuai, F. Alajaji, and G. Takahara, "Tight error bounds for nonuniform signaling over AWGN channels," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2712-2718, Nov. 2000.

[8] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[9] G. E. S´eguin, "A lower bound on the error probability for signals in white Gaussian noise," *IEEE Trans. Inform. Theory*, vol. 44, pp. 3168-3175, Nov. 1998.

[10] A. Viterbi and J. Omura, *Principles of Digital Communication and Coding.* Singapore: McGraw Hill, 1979.

TABLE I

SIZE GROWTH OF THE SUBSET $\mathcal{I}_1$ WITH SNR FOR THE LB-S BOUND AND COMPARISON OF THE KAT (WITH THE UPPER BOUND ON ρ_{ij}) AND LB-S BOUNDS FOR THE BCH (63, 10) CODE. $s_{\max}$ IS THE LARGEST WEIGHT AND $B_{s_{\max}}(\mathcal{I}_1)$ IS ITS CORRESPONDING NUMBER OF CODEWORDS IN $\mathcal{I}_1$.

E_b/N_0 (dB)	KAT (LB-s($\mathcal{C}$))	LB-s($\mathcal{I}_1$)	max. weight $s_{\max}$	$B_{s_{\max}}(\mathcal{I}_1)$	size of $\mathcal{I}_1$
-5	1.523016e-01	2.010236e-01	27	196	196
2	2.622454e-03	3.868599e-03	27	196	196
3	7.576149e-04	1.024943e-03	28	1	197
4	1.494706e-04	1.832994e-04	28	252	448
6	7.295594e-07	7.402885e-07	31	63	511
7	8.437699e-09	8.443873e-09	32	63	574
8	2.762258e-11	2.762258e-11	36	196	1022

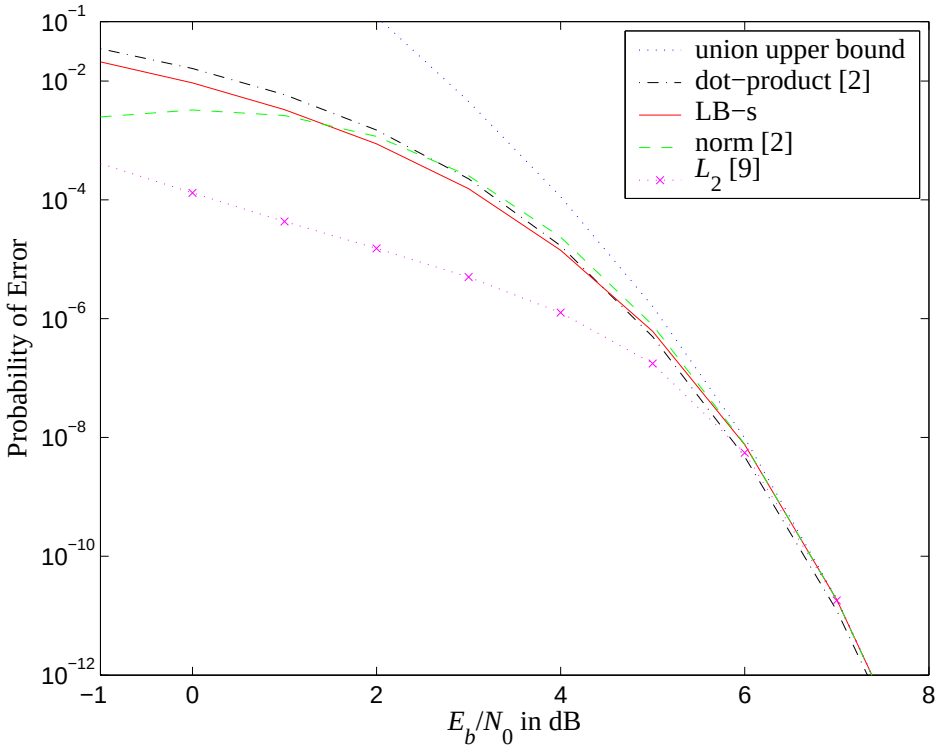

Fig. 1. Performance of various lower bounds for the BCH (63, 24) code. For reference, the union upper bound is also shown.

TABLE II

COMPARISON OF THE L_2, DOT-PRODUCT, NORM, AND THE LB-S LOWER BOUNDS FOR THE BCH (63, 24) CODE AND HIGH SNR VALUES. THE COMPUTATION TIME (IN SECONDS) OF THE BOUNDS FOR AN SNR RANGE FROM -5 TO 10 DB (WITH 1 DB INCREMENTS) ARE GIVEN IN PARENTHESIS. FOR REFERENCE, THE UNION UPPER BOUND IS ALSO PROVIDED.

E_b/N_0 (in dB)	L_2 (71) [9]	dot-product (15) [2]	norm (32076) [2]	LB-s (4)	union upper bound (< 1)
7	1.803442e-11	1.223649e-11	1.835702e-11	1.864105e-11	1.925149e-11
8	8.629289e-15	6.623727e-15	8.629879e-15	8.644060e-15	8.658352e-15
9	6.021990e-19	5.225418e-19	6.021990e-19	6.022246e-19	6.022503e-19
10	3.917180e-24	3.672375e-24	3.917180e-24	3.917182e-24	3.917184e-24

TABLE III

COMPARISON OF THE L_2, TIGHTENED L_2, DOT-PRODUCT, NORM, AND THE LB-S LOWER BOUNDS FOR THE GOLAY (24, 12) CODE AND HIGH SNR VALUES. THE COMPUTATION TIME (IN SECONDS) OF THE BOUNDS FOR AN SNR RANGE FROM -5 TO 10 DB (WITH 1 DB INCREMENTS) ARE GIVEN IN PARENTHESIS. FOR REFERENCE, THE UNION UPPER BOUND IS ALSO PROVIDED.

E_b/N_0 (in dB)	L_2 (1) [9]	L_2-s (2)	dot-product (15) [2]	norm (508) [2]	LB-s (1)	union upper bound (< 1)
7	7.982234e-08	8.001796e-08	8.219344e-08	8.462450e-08	8.504328e-08	9.181621e-08
8	4.470115e-10	4.470614e-10	4.470614e-10	4.490443e-10	4.522339e-10	4.576619e-10
9	5.930224e-13	5.930236e-13	5.930236e-13	5.930812e-13	5.937436e-13	5.944673e-13
10	1.420683e-16	1.420683e-16	1.420683e-16	1.420683e-16	1.420784e-16	1.420885e-16