Improved Lower Bounds for the Error Rate of Linear Block Codes*

Firouz Behnamfar, Fady Alajaji, and Tamás Linder

Department Mathematics and Statistics
Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario Canada K7L 3N6
{firouz, fady, linder}@mast.queensu.ca

Abstract

We obtain two lower bounds on the error rate of linear binary block codes (under maximum likelihood decoding) over BPSK-modulated AWGN 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. Two variations of the KAT lower bound are then derived. The first bound, the LB-f bound, requires the weight of the product of the codewords with minimum weight in addition to their weight enumeration, while the other bound, the LB-s bound (which is the main contribution of this paper), is algorithmic and only needs the weight enumeration function of the code. The use of a subset of the codebook to evaluate the KAT lower bound not only reduces computational complexity, but also tightens this bound specially at low signal-to-noise (SNR) ratios. Numerical results for binary block codes indicate that at low SNRs the LB-f bound is tighter than the LB-s bound. 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 original KAT bound (evaluated on the entire codebook), and the dot-product and norm bounds due to Cohen and Merhav.

1 Introduction

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

$$P(\mathcal{E}) = \sum_{u=0}^{M-1} P\left(\mathcal{E}|\boldsymbol{s}_u\right) p(\boldsymbol{s}_u), \tag{2}$$

*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.

where $\mathcal{E}$ is the codeword error event, $\boldsymbol{s}_u$ is the (modulated) signal corresponding to codeword $\boldsymbol{c}_u$, and $P(\mathcal{E}|\boldsymbol{s}_u)$ is the conditional probability of error given that $\boldsymbol{s}_u$ is transmitted. The computational complexity of evaluating the error rate via (2) is prohibitive even for moderate codebook sizes. For linear block codes under maximum likelihood (ML) detection 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 (AWGN) channels and binary phase-shift keying (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 $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-x^2/2} dx$ 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 and $N_0/2$ being the variance of the AWGN), r_c is the channel code rate, $w_i \triangleq w(\boldsymbol{c}_i)$ is the Hamming weight of codeword $\boldsymbol{c}_i$, and,

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

and $\boldsymbol{s}_0$ is the modulated version of the all-0 codeword. 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}

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

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

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

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 threefold. First, the L_2 bound depends only on the weight enumeration function of the code. 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

$$P(\mathcal{E}|\boldsymbol{s}_0) \geq \text{KAT}(\mathcal{C}) \triangleq \sum_{i\in\mathcal{C}, i\neq 0} \left(\frac{\theta_i Q^2(\sqrt{2\Delta w_i})}{\sum_{j\neq 0} \Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}) + (1-\theta_i) Q(\sqrt{2\Delta w_i})} + \frac{(1-\theta_i) Q^2(\sqrt{2\Delta w_i})}{\sum_{j\neq 0} \Psi(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}) - \theta_i Q(\sqrt{2\Delta w_i})} \right), \quad (8)$$

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 outperforms de Caen's bound by a factor of at most 9/8.

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 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].

2 The Tightened Lower Bounds

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

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

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 $\mathcal{S} \triangleq \{0, 1, ..., M-1\}$ is the index set of the codewords, $\mathcal{I}$ is a sub-collection of the codewords, and ϵ_{0i} is the event that between codewords $\boldsymbol{s}_i$ and $\boldsymbol{s}_0$, $\boldsymbol{s}_i$ is decoded at the receiver. The problem becomes now to determine a "good" subset $\mathcal{I}$ 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. Hence, as noted in [2] (see also the references therein), a natural candidate for the subset $\mathcal{I}$ is the set of the codewords with minimum weight $D_{\min}$. The resulting bound, hereafter denoted by LB-f, is given by

$$P\left(\mathcal{E}|\boldsymbol{s}_0\right) \geq \text{LB-f} \triangleq \sum_{k\in\mathcal{S}:w_k=D_{\min}} \left(\frac{\theta_k Q^2(\sqrt{2\Delta D_{\min}})}{S_1 + Q\left(\sqrt{2\Delta D_{\min}}\right)} + \frac{(1-\theta_k)Q^2(\sqrt{2\Delta D_{\min}})}{S_1}\right), \tag{10}$$

where

$$S_1 = \sum_{j\in\mathcal{S}:w_j=D_{\min}} \Psi\left(\rho_{kj}, \sqrt{2\Delta D_{\min}}, \sqrt{2\Delta D_{\min}}\right) - \theta_k Q\left(\sqrt{2\Delta D_{\min}}\right).$$

This bound is significantly less complex than the original KAT bound in (8), because it only employs the minimum-weight codewords which form a relatively small subset of the codebook. We note that in addition to the weight enumeration function, this bound requires the weight of the product of the codeword pairs to compute ρ_{kj} (see (5)). Note also that no maximization is performed to obtain the LB-f lower bound.

To derive the second bound, we first use the upper bound on ρ_{ij} which is given in (6) so that this bound can be calculated using only the weight enumeration function (which is readily available). We also want the bound to be computationally efficient, therefore we only evaluate (8) on a subset $\mathcal{I}$ (instead of $\mathcal{C}$). The main issue now is that replacing ρ_{ij} with κ_{ij} results in an upper bound for the $\Psi(\cdot,\cdot,\cdot)$ functions in (8) which could make (11) a lower bound to (8). However, using the upper bound for ρ_{ij} will also change the value of θ_i in (8) into $\tilde{\theta}_s$ in (11), so we need to prove that the LB-s is still a lower bound for $P\left(\mathcal{E}|\boldsymbol{s}_0\right)$. We therefore obtain the following Lemma.

Lemma – Consider a liner 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 $\mathcal{I}$. A lower bound for the error rate of the code is given by

$$P\left(\mathcal{E}\right) = P\left(\mathcal{E}|\boldsymbol{s}_0\right) \geq \text{LB-s}(\mathcal{I}) \triangleq$$
$$\sum_{s=1}^{n} B_s(\mathcal{I}) Q^2(\sqrt{2\Delta s}) \left(\frac{\tilde{\theta}_s}{(2-\tilde{\theta}_s)Q(\sqrt{2\Delta s}) + S_2} + \frac{1-\tilde{\theta}_s}{(1-\tilde{\theta}_s)Q(\sqrt{2\Delta s}) + S_2}\right), \tag{11}$$

where

$$S_2 = (B_s(\mathcal{I}) - 1)\Psi\left(1 - \frac{D_{\min}}{2s}, \sqrt{2\Delta s}, \sqrt{2\Delta s}\right) + \sum_{t \neq 0,s} B_t(\mathcal{I})\Psi(\kappa_{st}, \sqrt{2\Delta s}, \sqrt{2\Delta t}),$$

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.

Two 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.

Since the LB-s bound is expressed in terms of κ_{st}, it only needs the codeword weights for its evaluation. We next propose an algorithm to tighten the LB-s lower bound (for a given SNR) by iteratively enlarging the sub-collection of codewords. The algorithm consists of the following steps:

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.

The computational complexity of the LB-s bound is very favorable as compared with the dot-product and norm bounds of [2] which need to find other parameters via exhaustive search. 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 observed to be optimal. Moreover, the LB-s bound is observed to be over an order of magnitude larger than the KAT bound computed using (6) at low SNRs.

One may note that the above algorithm can still be too tedious for very large codebooks. We therefore slightly modify Step 2 of the above algorithm as

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

This new step requires the algorithm to be run for at most n times (and in fact for much less than that) instead of $2^k - 1$ times, resulting in drastic savings in the run time.

3 Numerical Results

We first compare the tightness of the various KAT bounds. Figure 1 shows the original KAT bound in (8) (using the upper bound on ρ_{ij} in (6)), LB-f, and LB-s lower bounds for the error rate of the BCH (15, 11) code. The union upper bound is also plotted for comparison. It is observed that if the weight of the products of the minimum-weight codewords is available, then the LB-f bound should be chosen. The LB-s bound is also tighter than the original KAT bound

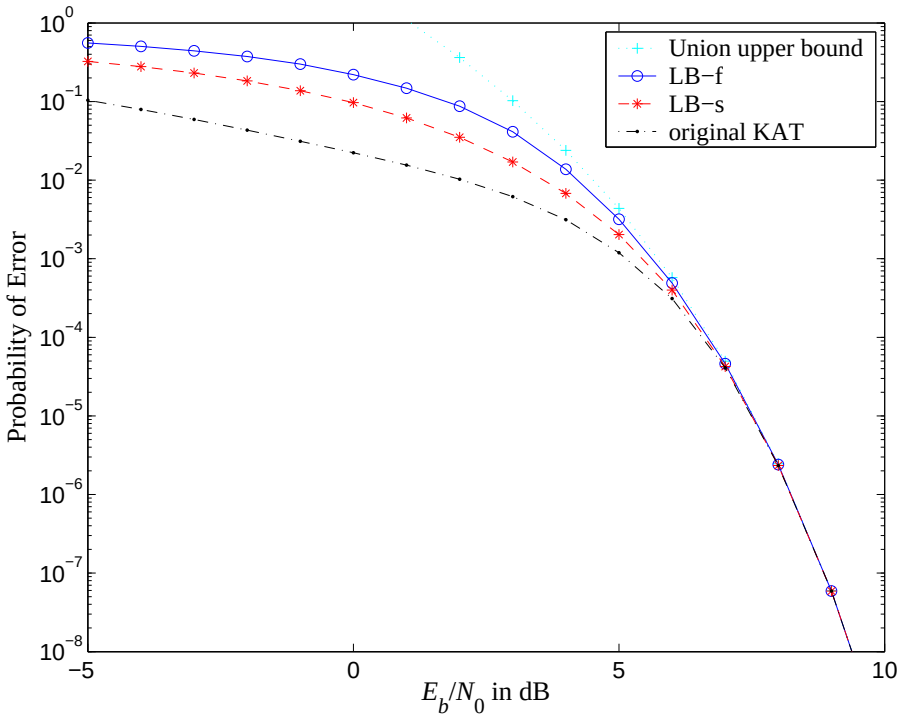

Figure 1: Comparisons among the original KAT (using the entire codebook), LB-s, and LB-f bounds for the BCH (15, 11) code. For reference, the union upper bound is also shown.

particularly at low SNRs. Table 1 also compares the L_2, original KAT, and LB-s lower bounds for the BCH (15, 7) code and confirms the superiority of the LB-s bound over the original KAT bound, which is in turn tighter than the L_2 bound. Note that, similar to Figure 1, the LB-s and original KAT bounds become exact (by converging to the union upper bound) as the SNR approaches infinity.

The gradual enlargement of the subset $\mathcal{I}_1$ used in LB-s (with respect to SNR) is demonstrated in Table 2 for the BCH (63, 10) code (the weight spectrum of the code is specified by $(s, B_s(\mathcal{I})) \in \{(0,1),(27,196),(28,252),(31,63),(32,63),(35,252),(36,196),(63,1)\}$). It is observed that the best codeword set $\mathcal{I}_1$ grows with the SNR, reducing the gap between its corresponding LB-s bound and the LB-f bound. At moderate SNRs (6 dB for this example), the LB-s bound outperforms the LB-f bound because the LB-f lower bound only uses the minimum-weight codewords. Note that at high SNRs, the LB-s bound 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)).

Table 1: Comparison of the LB-s bound with the L_2 [9] and the original KAT lower bounds for the BCH (15, 7) code.

E_b/N_0 (dB)	L_2 [9]	original KAT	LB-s
-5	0.1952191	0.1952347	0.2985750
0	0.0445509	0.0445904	0.0782395
5	7.68260e-4	8.27783e-4	9.25403e-4
10	7.67117e-11	7.67682e-11	7.67682e-11

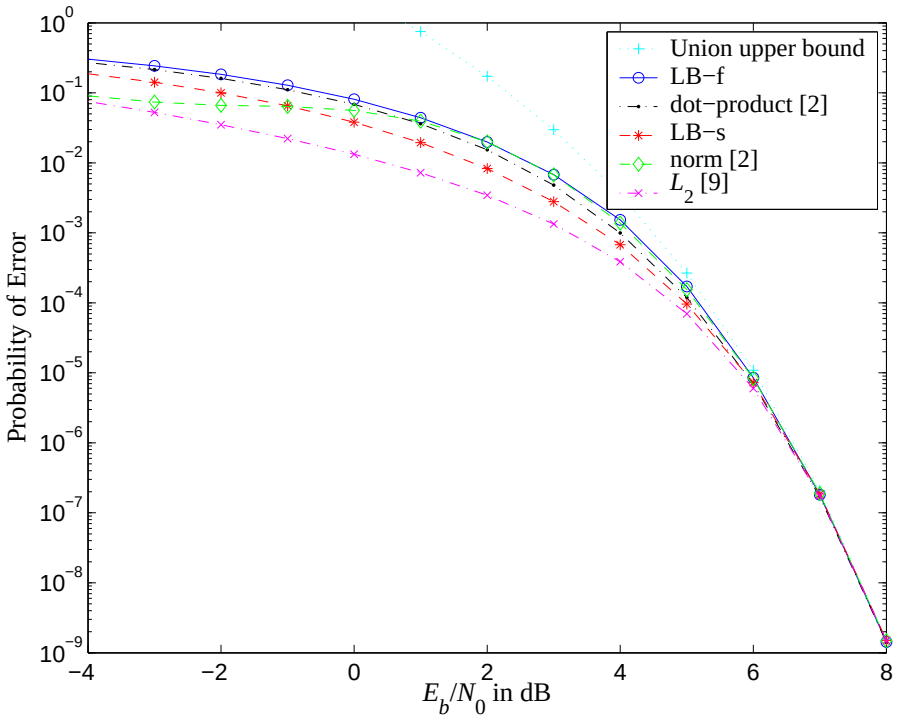

Figure 2: Performance of various lower bounds for the Golay (23, 12) code. For reference, the union upper bound is also shown.

Figure 2 compares the performance of the L_2, dot-product, norm, LB-f, and LB-s bounds for the Golay (23, 12) code. At low SNRs, the LB-f bound outperforms the other bounds. If the exact value of ρ_{ij} is not available, then, for SNR $\leq$ 0 dB, the dot-product bound of [2] is the tightest bound among the above bounds. As the SNR grows, the LB-s bound becomes the largest (tightest) bound. Table 4 emphasizes this point for SNR $>$ 6 dB and the BCH (15, 11) code: the LB-s bound is observed to be tighter than the other bounds for the entire SNR range considered in the table.

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 Section 2 drastically reduces the computation time for the LB-s bound. For example, as shown in Table 3, the run time of the norm bound in the -5

Table 2: Size growth of the subset $\mathcal{I}_1$ with SNR for the LB-s bound and 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)	LB-f	LB-s	max. weight $s_{\max}$	$B_{s_{\max}}(\mathcal{I}_1)$	size of $\mathcal{I}_1$
-5	2.394711e-01	2.010236e-01	27	196	196
2	5.615240e-03	3.868599e-03	27	196	196
3	1.493219e-03	1.024943e-03	28	1	197
4	2.435199e-04	1.832994e-04	28	252	448
6	4.945912e-07	7.402885e-07	31	63	511
7	5.453444e-09	8.443873e-09	32	63	574
8	1.883346e-11	2.762258e-11	36	196	1022

Table 3: 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 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

to 10 dB range (with 1 dB increments) is 32076 seconds (i.e., more than 8.9 hours) on a SUN UltraSparc platform, while it is 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). 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 of the same order of magnitude. 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.

We have repeated the algorithm of Section 2 for the L_2 bound to obtain a tighter version of this bound, referred to as the L_2-s bound, and reported the results in Table 4 (it can be verified that L_2-s is also 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 is never tighter than the norm bound of [2] or the LB-s bound derived here. The subsets used by the L_2-s bound are in general observed to be slightly different than those used by the LB-s bound. As the SNR grows, all of the bounds in Table 4 (except for the dot-product bound) use larger subsets. At high SNRs (> 9 dB in this case), all of the bounds use the entire codebook; so it is fair to compare the ratios of the norm and LB-s bounds to the L_2-s bound (from Section 2 recall that the ratio of the LB-s bound to the L_2-s bound is at most 9/8 = 1.125). The ratio is 1.003 at 9 dB for the norm bound, while it is 1.01 for the LB-s bound. For low SNRs, where the L_2-s, norm, and LB-s bounds use their own optimal subsets which may be different in general, the 9/8 ratio does not hold anymore. It is interesting to note that the LB-s bound provides even a better improvement over the L_2 bound as compared with the norm bound. For example, at SNR = 6 dB, the ratio of the LB-s bound to the L_2 bound is 1.383 while this ratio reduces to 1.352 for the norm bound. A similar behavior is observed for other linear block codes.

4 Conclusions

We derived two simple lower bounds on the error probability of ML decoded block codes based on the KAT lower bound. One of the bounds, denoted by LB-f, has the drawback of requiring the knowledge of the weight of the product of pairs of codewords with minimum weight. The other bound, which is the main contribution of this paper and is denoted by LB-s, is algorithmic and 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 LB-f and the other lower bounds considered in this paper at high SNRs.

The results of this paper were presented for the AWGN channel. Nevertheless, they can be

Table 4: Comparison among L_2, tightened L_2 (L_2-s), dot-product, norm, and the LB-s lower bounds for the BCH (15, 11) code and medium to high SNR values. For reference, the union upper bound is also provided.

E_b/N_0 (in dB)	L_2 [9]	L_2-s	dot-product [2]	norm [2]	LB-s	union upper bound
6	2.8899e-4	3.5696e-4	3.7164e-4	3.9058e-4	3.9966e-4	5.7507e-4
7	3.7276e-5	3.9677e-5	4.0215e-5	4.1464e-5	4.2480e-5	4.9636e-5
8	2.2487e-6	2.2649e-6	2.2649e-6	2.3029e-6	2.3353e-6	2.4631e-6
9	5.8356e-8	5.8365e-8	5.8226e-8	5.8535e-8	5.8958e-8	5.9645e-8
10	5.7342e-10	5.7342e-10	5.7276e-10	5.7354e-10	5.7451e-10	5.7564e-10

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

$$\sum_i Q\left(\sqrt{2\Delta w_i}\right) g(K_i, \theta_i), \tag{12}$$

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

$$\sum_j \Psi\left(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) = (K_i + \theta_i) Q\left(\sqrt{2\Delta w_i}\right). \tag{13}$$

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, (12) still gives a lower bound for $P\left(\mathcal{E}|\boldsymbol{s}_0\right)$. To this end, we first let

$$\sum_j \Psi\left(\kappa_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) = (\tilde{K}_i + \tilde{\theta}_i) Q\left(\sqrt{2\Delta w_i}\right), \tag{14}$$

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

$$g(K_i, \theta_i) \geq g(\tilde{K}_i, \tilde{\theta}_i). \tag{15}$$

From $\Psi\left(\kappa_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right) \geq \Psi\left(\rho_{ij}, \sqrt{2\Delta w_i}, \sqrt{2\Delta w_j}\right)$, (13), and (14), it follows that

$$\tilde{K}_i + \tilde{\theta}_i \geq K_i + \theta_i. \tag{16}$$

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 (16) 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, (15) 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

$$g(\tilde{K}_i, \tilde{\theta}_i) - g(K_i, \theta_i) = \frac{K_i(K_i + 1)(\tilde{K}_i + 1) - (K_i + 1)\tilde{K}_i(\tilde{K}_i + 1) + \theta_i \tilde{K}_i(\tilde{K}_i + 1) - \tilde{\theta}_i K_i(K_i + 1)}{K_i(K_i + 1)\tilde{K}_i(\tilde{K}_i + 1)}. \quad (17)$$

The denominator of (17) 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), (15) also holds for the second case. This completes the proof of (15).

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. Séguin, "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.