Bounds on the Average Binary Minimum Distance and the Maximum Likelihood Performance of Reed Solomon Codes*

Mostafa El-Khamy
California Institute of Technology
1200 E California Blvd.
Pasadena, CA 91125
mostafa@systems.caltech.edu

Robert J. McEliece
California Institute of Technology
1200 E California Blvd.
Pasadena, CA 91125
rjm@systems.caltech.edu

Abstract

In this paper, an average binary weight enumerator of Reed Solomon (RS) codes is derived assuming a binomial distribution of the bits in a non-zero symbol. Lower bounds on the average binary minimum distance are shown. The averaged binary image of the RS code is shown to be asymptotically good for sufficiently high rates. These results are used to bound the maximum likelihood performance of RS codes, whose binary image is modulated using binary phase shift keying on AWGN channels, for both hard and soft decision decoding.

1 Introduction

Reed Solomon (RS) codes are one of the most important codes due to their wide variety of applications ranging from data storage to satellite communications. Decoding of RS codes has received wide attention lately (c.f. [1–5]). The optimum hard decision decoder is the maximum likelihood (ML) decoder. However, it has been shown in [6] that ML decoding of a general linear code is NP (nondeterministic polynomial time) hard. Recently, this was also shown specifically for RS codes in [7]. Thus, it is important to compare the performance of polynomial-time decoding algorithms with the performance of the optimum ML decoder. For both soft and hard decision decoding algorithms, the corresponding ML decoder provides a benchmark to compare the performance of other suboptimum algorithms. In this paper we focus on bounding the performance of optimum ML decoding when the binary image of the RS code is modulated using binary phase shift keying (BPSK) [8] and transmitted over an additive white Gaussian noise (AWGN) channel. Let $\boldsymbol{x} = \mathcal{M}(\boldsymbol{u}) = 1 - 2\boldsymbol{u}$ be the BPSK modulation of the binary image $\boldsymbol{u} \in \mathbb{C}$ of an (n, k) codeword, then the received vector is $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$, where $\boldsymbol{z}$ is an AWGN vector. Since the considered codes are linear, it is safe to assume that the all zero codeword (in fact its binary image) is transmitted. The analysis will depend on the number of codewords within a certain Hamming distance from the all zero codeword. Thus, the bounds depend mainly on the binary weight enumerator (BWE) of the used

*This research was supported by NSF grant no. CCR-0118670 and grants from Sony, Qualcomm, and the Lee Center for Advanced Networking

code, which in turn depends on the basis used to represent the symbols in GF(q) as bits . Bounds on the performance of binary block codes transmitted over AWGN channels were studied in the literature [8–10]. The problem of applying them to bound the performance of RS codes is actually the problem of finding the BWE of the RS code. For particular realizations of RS codes, the BWE as well as enumerating the codewords by the number of symbols of each kind in each codeword were studied (see for example [11, 12]). The average BWE of Generalized Reed Solomon (GRS) codes, derived from an original RS code either by using a different basis to expand each column in the RS generator matrix into a binary representation or by multiplying each column in the RS generator matrix by some non-zero element in GF(2^m), was studied in [13]. Since the BWE of the RS code is not unique, we approximate the BWE of an RS code with an averaged BWE. (This technique could also be applied to other codes.) This is shown in Sec. 2 and we also justify this approximation. The performance of the code at large signal to noise ratios is determined by its minimum distance.

Although the symbol minimum distance of an (n, k, d) RS code is $d = n - k + 1$, the binary minimum distance is not known. The binary minimum distance of an RS code depends on how the q-ary symbols are represented as bits. Thus, we derive lower bounds on the averaged binary minimum distance in Sec. 3. We give a bound on the minimum rate at which the average binary minimum distance is equal to the symbol minimum distance and show that for higher rates the averaged binary image of an RS code asymptotically satisfies the Gilbert-Varsharmov (GV) bound. Using the averaged BWE, the performance of RS codes, whose binary image is BPSK modulated over an AWGN channel, is analyzed in Sec. 4 for both hard and soft decision ML decoders.

2 Average Binary Weight Enumerator of RS Code

The symbol weight enumerator function of an (n, k, d) code $\mathbb{C}$ over GF(2^m) is defined to be $A(x) = \sum_{i=0}^{n} A_i x^i$, where A_i is the number of codewords with symbol Hamming weight i. The binary image of the code is obtained by representing each symbol in GF(2^m) by an m-dimensional binary vector in terms of a basis of the field [14]. Assuming that the distribution of ones and zeros in the m-dimensional binary image of a non-zero symbol follows a binomial distribution, the probability of having i ones in a non-zero symbol is $\frac{1}{2^m-1}\binom{m}{i}$. The generating function of the *average* BWE of a non-zero symbol is

$$G_s(x) = \sum_{i=1}^{m} \frac{1}{2^m - 1}\binom{m}{i} x^i = \frac{(1+x)^m - 1}{2^m - 1}, \tag{1}$$

where the power of x denotes the binary weight and the all zero symbol is excluded since the binary weight is at least one. Suppose a codeword has w non-zero symbols, and the distribution of the ones and zeros in each symbol is independent from other symbols, then the possible binary weight, b, of this codeword ranges from w to mw. Since there are A_w codewords with symbol Hamming weight w, then the average binary weight enumerator function is

$$G(x) = A(y)|_{y=G_s(x)} = \sum_{w=0}^{n} A_w (G_s(x))^w = \sum_{b=0}^{nm} G_b x^b, \tag{2}$$

where

$$G_b = \sum_{w=d}^{n} \frac{A_w}{(2^m - 1)^w} \sum_{j=0}^{w} (-1)^{w-j} \binom{w}{j} \binom{jm}{b}; \quad b \geq d. \tag{3}$$

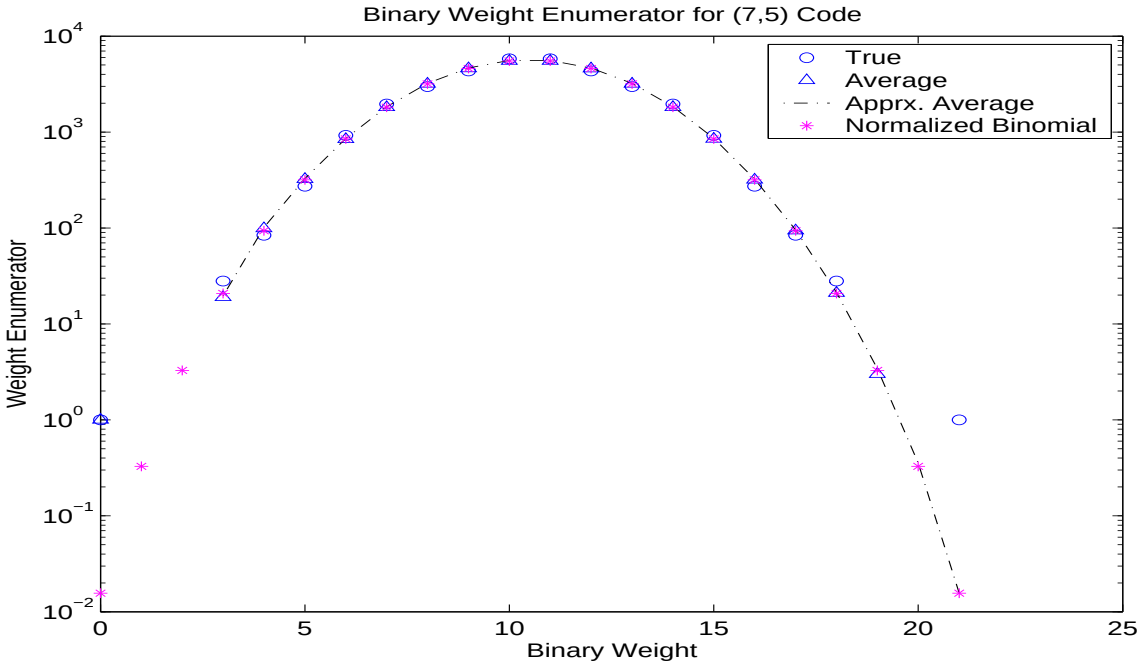

Figure 1: True BWE versus the averaged BWE for the (7,5) RS code

The symbol weight enumerator of an (n, k, d) RS code over GF(q) is [15, Th. 25.7]

$$A_j = \binom{n}{j}(q-1)\sum_{i=0}^{j-d}(-1)^i\binom{j-1}{i}q^{j-i-d}; \quad j \geq d. \tag{4}$$

(The results in this paper apply to any q-ary maximum distance separable (MDS) code, where $q = 2^m$ and not necessarily an RS code.) Widely used RS (MDS) codes have a code length $n = 2^m - 1$. In that case the BWE derived in (3) agrees with the average BWE of a class of GRS codes [13]. It is easy to see that $G_o = 1$ and that $G_b = 0$ for $0 < b < d$. By substituting for A_w, for $b \geq d$,

$$G_b = \sum_{w=d}^{n}(q-1)\left(\frac{q}{q-1}\right)^w\binom{n}{w}\sum_{v=0}^{w-d}(-1)^v\binom{w-1}{v}\left[\sum_{j=\lceil b/m\rceil}^{w}(-1)^{w-j}\binom{w}{j}\binom{jm}{b}q^{-(d+v)}\right]. \tag{5}$$

However, the term $\binom{jm}{b}$ may diverge numerically for large j. Using the Stirling approximation for $\binom{jm}{b}$ [16], the function G_b could be approximated as

$$G_b \approx \sum_{w=d}^{n}(q-1)\left(\frac{q}{q-1}\right)^w\binom{n}{w}\sum_{v=0}^{w-d}(-1)^v\binom{w-1}{v}\sum_{j=\lceil b/m\rceil}^{w}\mathcal{F}(j), \tag{6}$$

where

$$\mathcal{F}(j) = \begin{cases} (-1)^{w-j}\binom{w}{j}2^{\lambda(j)}; & j > b/m \\ \\ (-1)^{w-j}\binom{w}{j}2^{-m(d+v)}; & j = b/m \end{cases}, \tag{7}$$

and $\lambda(j) = m(jH(\psi_{b,j}) - d - v) - \frac{1}{2}\log_2\left(2\pi jm\psi_{b,j}(1-\psi_{b,j})\right)$ for $\psi_{b,j} = b/jm$ and $q = 2^m$. This approximation could be further simplified by using the fact that $1 \leq \left(\frac{q}{q-1}\right)^w \leq e$ and substituting in (6).

In Fig(1), the averaged BWE and the true BWE for a specific basis representation (found by computer search in [17]) are plotted for the $(7, 5)$ RS code over $GF(8)$. The approximation of (6) is labeled 'Apprx. Average'. It is observed that the average BWE closely approximated the true BWE for this basis representation. The average BWE is found to be very close to a binomial enumerator, normalized such that the cardinality of $\mathbb{C} = q^k$, $\hat{G}_b = q^{-(n-k)}\binom{mn}{b}$. (This could be justified by the central limit theorem.)

3 Lower Bounds on the Average BMD of RS Codes

The error correcting capability of a code relies a lot on the minimum distance of the code. The actual average minimum distance of the binary image of the RS code could be defined as the smallest weight b whose average BWE G_b is greater than or equal to one (note that G_b is a real number). The binary minimum distance (BMD) is at least as large as the symbol minimum distance d. Let d_b be the average BMD, then

$$d_b = \inf_{b \geq d}\{b : G_b \geq 1\}. \tag{8}$$

The number d_b could be found exactly by computer search. However it will be useful to find a lower bound (LB) on d_b. (A trivial lower bound is $d_b \geq d$.)

An upper bound on the symbol weight enumerator A_j is [18, Eq. 12]

$$A_j \leq \binom{n}{j}(q-1)^{j-d+1}; \quad j \geq d. \tag{9}$$

Substituting in (3) it follows that,

$$G_b \leq (q-1)^{k-n}\sum_{w=d}^{n}\binom{n}{w}\left[\sum_{j=\lceil b/m\rceil}^{w}(-1)^{w-j}\binom{w}{j}\binom{jm}{b}\right]. \tag{10}$$

The term $\binom{jm}{b}$ is upper bounded as $\binom{jm}{b} \leq \frac{j^b m^b}{b!}$. If b is relatively small compared to jm, or asymptotically as $jm \to \infty$, we have $\binom{jm}{b} \sim \frac{j^b m^b}{b!}$. The approximation is valid for sufficiently high rates, R, where $d = n(1 - R + 1/n)$ is relatively small, and consequently $b = d_b$ is also small. G_b is approximately upper bounded by

$$\frac{m^b}{b!}(q-1)^{k-n}\sum_{w=d}^{n}\binom{n}{w}\left[\sum_{j=0}^{w}(-1)^{w-j}\binom{w}{j}j^b\right] = \tag{11}$$

$$\frac{m^b}{b!}(q-1)^{k-n}\sum_{w=d}^{n}\binom{n}{w}\mathbb{S}(b,w)w!, \tag{12}$$

where $\mathbb{S}(b, w)$ is the Stirling number of the second kind [15] and satisfies the recurrence relation $\mathbb{S}(n, k) = k\mathbb{S}(n-1, k) + \mathbb{S}(n-1, k-1)$ with $\mathbb{S}(0, 0) = 1$.

By rearranging and the definition of G_b, it follows that an approximate lower bound on d_b is

$$\inf_{b \geq d}\left\{b : \frac{m^b}{b!}\sum_{w=d}^{n}\binom{n}{w}\mathbb{S}(b,w)w! \geq (q-1)^{d-1}\right\}. \tag{13}$$

The LB of (13) could be solved numerically and it does not require evaluating the symbol weight enumerator for all possible weights as evaluating G_b does. This bound

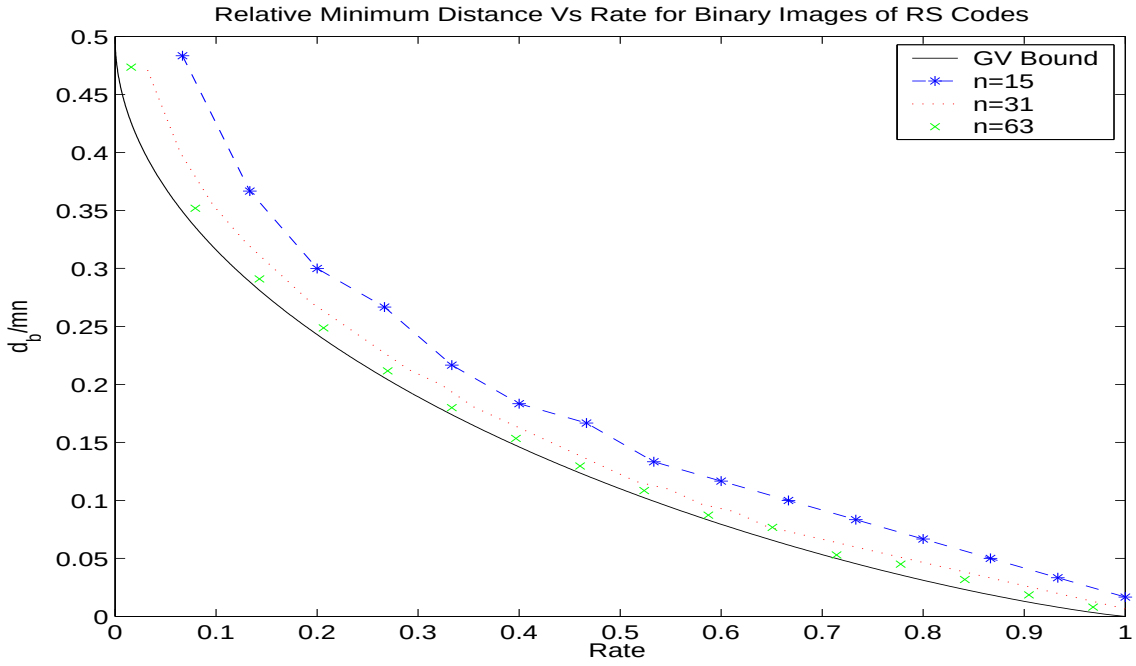

Figure 2: Relative average BMD for codes of different length versus the code rate.

could also be simplified by starting the summation in (12) over w from 0 instead of d and splitting it into two summations, it follows that G_b is (approximately) upper bounded by

$$\frac{m^b(q-1)^{1-d}}{b!}\left[\sum_{w=0}^{b}\binom{n}{w}\mathbb{S}(b,w)w! + \sum_{w=b+1}^{n}\binom{n}{w}\mathbb{S}(b,w)w!\right]. \tag{14}$$

Since $\mathbb{S}(n,k)$ is the number of partitions of an n-element set into k non-empty sets, then $\mathbb{S}(n,k)=0$ if $k>n$. This implies that the second summation is zero. From the definition of the Stirling's number [15, Th. 13.5], it follows that $n^b=\sum_{w=0}^{b}\binom{n}{w}\mathbb{S}(b,w)w!$. Thus the upper bound (14) is equivalent to $\frac{m^b n^b}{b!}(q-1)^{1-d}$. Using $G_{d_b}\geq 1$, an approximate lower bound on d_b is given by

$$\inf_{b\geq d}\left\{b:\frac{(mn)^b}{b!}\geq(q-1)^{d-1}\right\}. \tag{15}$$

By taking only the term corresponding to $j=w$ in the alternating sign summation in (10), if follows that

$$G_b\leq(q-1)^{k-n}\sum_{w=d}^{n}\binom{n}{w}\binom{wm}{b}\leq(q-1)^{k-n}\binom{n}{\lfloor n/2\rfloor}\sum_{h=b}^{mn}\binom{h}{b}. \tag{16}$$

An exact lower bound is thus given in the following lemma.

Lemma 1 *A lower bound on d_b is*

$$d_b\geq\inf_{b\geq d}\left\{b:\binom{mn+1}{b+1}\geq\frac{(q-1)^{n-k}}{\binom{n}{\lfloor n/2\rfloor}}\right\}. \tag{17}$$

It is interesting to determine the minimum rate R for a given code length at which the average BMD is equal to the symbol minimum distance d which is linear in R. This is stated in the following lemma.

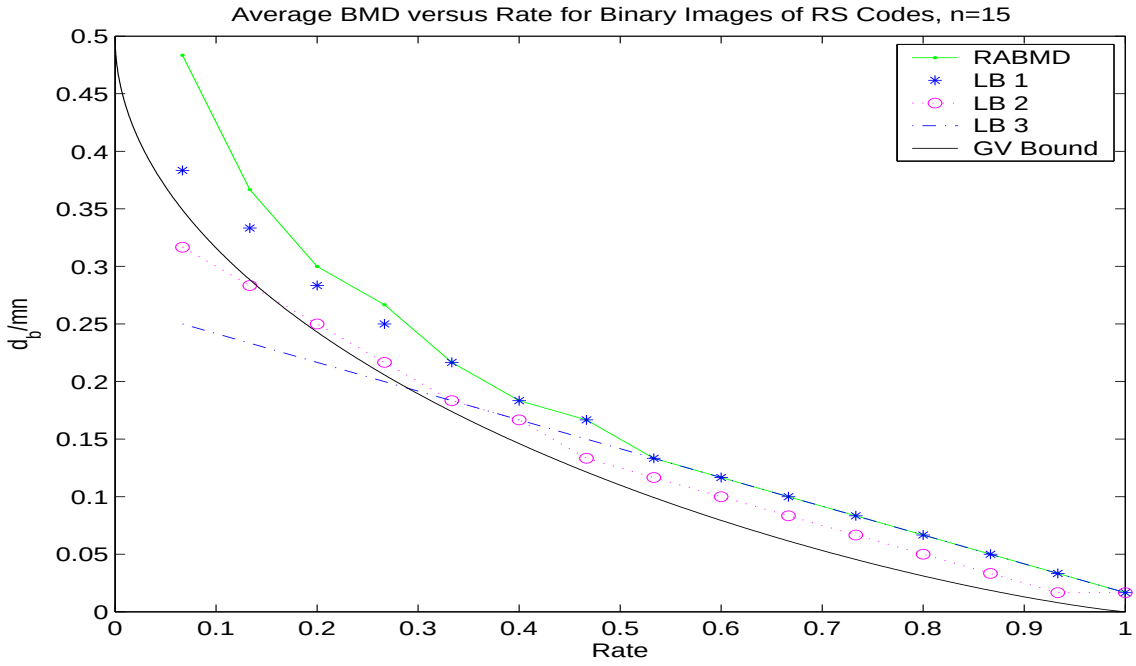

Figure 3: Relative average binary minimum distance for n=15 and q=16.

Lemma 2 *The average BMD is equal to the symbol minimum distance for all rates greater than or equal to* $R_o = 1 - \frac{d_o - 1}{n}$ *where* d_o *is the largest integer* d *such that*

$$\frac{1}{d}\log_2\left((q-1)\binom{n}{d}\right) \geq \log_2(q-1) - \log_2(\log_2(q)). \tag{18}$$

Proof: The number of codewords in an MDS code with symbol weight $d = n - k + 1$ is $A_d = (q-1)\binom{n}{d}$. The binary image could be of binary weight d only if the codeword is of symbol weight d and the binary representation of each non-zero symbol has only one non-zero bit. This happens with probability $\left(\frac{m}{2^m - 1}\right)^d$, where $m = \log_2(q)$. So the average number of codewords with binary weight d is

$$G_d = A_d\left(\frac{m}{2^m - 1}\right)^d = (q-1)\binom{n}{d}\left(\frac{\log_2(q)}{q-1}\right)^d. \tag{19}$$

From the definition of the average BMD, the lemma follows. ■

In [13], Retter showed that for sufficiently large code lengths, most GRS codes lie close to the GV bound by showing that the number of codewords with weights lying below the GV bound in all GRS codes of the same length and rate are less than half the number of such GRS codes. The GV bound is defined by [14],

$$\lim_{n\to\infty}\{R(\delta) - (1 - H(\delta))\} \geq 0 \;\text{ for }\; 0 < \delta < \frac{1}{2}, \tag{20}$$

where $\delta = d_b/(mn)$ is the ratio of the binary minimum distance to the total length of the code, H is the binary entropy function and $R(\delta)$ is the corresponding code rate. We show a related result for a RS code with an averaged BWE G_b in the following lemma.

Lemma 3 *The average binary image of the RS code asymptotically satisfies the GV bound for all rates* $R \geq R_o$ *where* R_o *is defined in Lem.(2).*

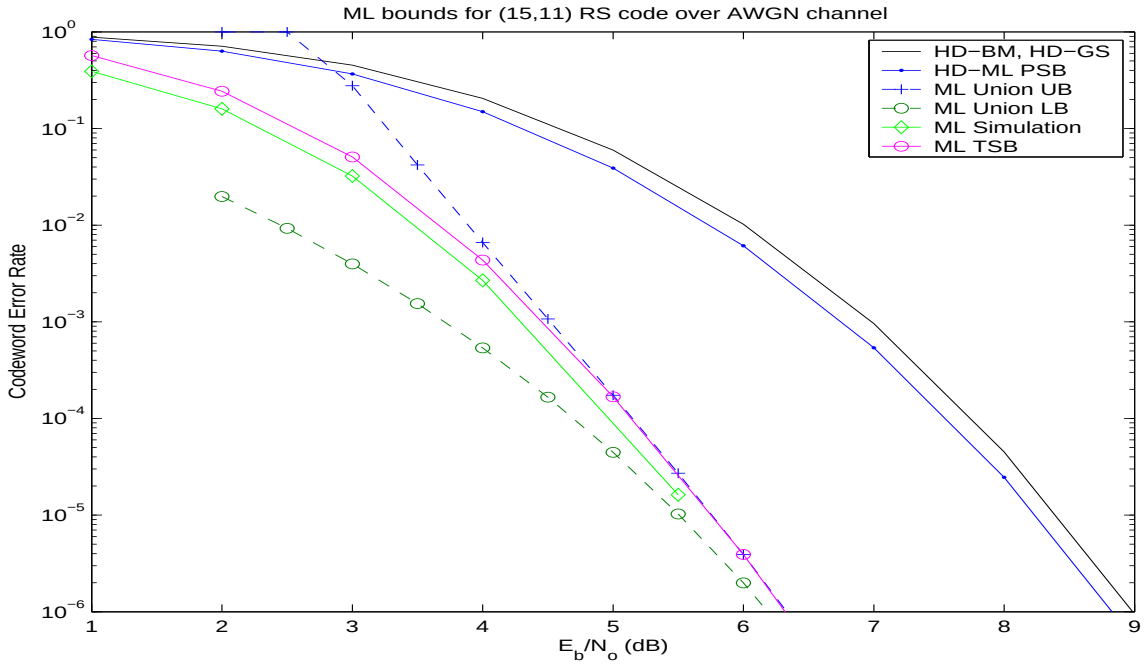

Figure 4: Performance bounds of the $(15, 11)$ RS code, $q = 16$, over AWGN channels.

Proof: For $R \geq R_o$, $d_b = d$ and $G_d = (q-1)\binom{n}{d}\left(\frac{m}{q-1}\right)^d \leq \alpha\binom{mn}{d}(q-1)^{1-d}$, where the last inequality follows from $\binom{n}{d}m^d \leq \frac{n^d m^d}{d!} \leq \alpha\binom{nm}{d}$, and $\alpha \to 1$ as $mn \to \infty$. (For $k \sim c\sqrt{n}$, $\binom{n}{k} \sim e^{-c^2/2}\frac{n^k}{k!}$ with a fixed positive real c.) Asymptotically as $n \to \infty$, and $\delta = d/mn$

$$1 \leq G_d \leq \alpha 2^{mn(H(\delta))}(q-1)^{1-d} \leq 2^{mn(H(\delta))}\alpha q^{1-d}e. \tag{21}$$

Equivalently, $R(\delta) - (1 - H(\delta)) \geq -\frac{\log_2(\alpha)+1.4426}{mn} \geq -\epsilon$ where $\epsilon \to 0$ as $mn \to \infty$. ■

Note that this is for the average binary image of the RS code and not for a specific valid binary image. Asymptotically, it could be shown that R_o is the smallest rate such that $(H(1-R_o)/(1-R_o)) - \log(n) + \log(\log(n)) \geq 0$. This implies that R_o tends to one as n tends to infinity. It is also possible to show that if a code's binary minimum distance is lower bounded by (13), then, in the limit of large n, it will asymptotically satisfy the GV bound.

The lower bounds of (13), (15) and (17) are labelled 'LB1', 'LB2' and 'LB3' respectively. The GV bound, $R(\delta) = 1 - H(\delta)$, is labelled 'GV'. The relative average binary minimum distance (RABMD) $\delta = d_b/mn$ is plotted versus the rate of the code for $n = 15, 31$ and 63 in Fig. 2. It is observed that they satisfy the GV bound. The lower bounds as well as the RABMD and the GV bound are shown in Fig. 3 for $n = 15$. It is noticed that for $n = 15$ and $k \geq 8$, the average BMD is equal to the symbol minimum distance, d. This is expected from Lem. 2. For lower rate codes, the average BMD is greater than the symbol minimum distance. The bounds are tighter for high rates $(R \geq 0.5)$ as expected. For larger n and high rates, the approximate lower bounds LB1 and LB2 coincide with the GV bound. The difference between LB1 and LB2 is negligible for $n \geq 31$. The lower bound LB3 is tight at high rates. Moreover, it is much easier to evaluate the bounds than to actually search for the average binary minimum distance.

4 Performance of the Maximum Likelihood Decoders

Hard decision is done to the received bits to obtain the vector, $\hat{u}_i = \frac{1-\text{sign}(y_i)}{2}$ and the HD-ML decoder's output is the codeword $\boldsymbol{v'}$ such that

$$\boldsymbol{v'} = \arg_{\boldsymbol{v}} \min_{\boldsymbol{v} \in \mathbb{C}} \text{dist}(\hat{\boldsymbol{u}}, \boldsymbol{v}) \tag{22}$$

where $\text{dist}(\boldsymbol{u}, \boldsymbol{v})$ is the (binary) Hamming distance between $\boldsymbol{u}$ and $\boldsymbol{v}$. This is equivalent to transmitting the codeword $\boldsymbol{u}$ through a binary symmetric channel (BSC) with cross over probability $p = Q(\sqrt{2R\gamma})$ where γ is the bit signal to noise ratio. The HD-ML performance could be upper bounded by using the averaged BWE of the RS code, and the Poltyrev sphere bound (PSB) for linear codes over binary symmetric channels [9].

Optimum soft decision ML decoding of a code solves the following optimization problem,

$$\boldsymbol{v'} = \arg_{\boldsymbol{v}} \min_{\boldsymbol{v} \in \mathbb{C}} \|\boldsymbol{y} - \mathcal{M}(\boldsymbol{v})\|^2 \tag{23}$$

where $\|\boldsymbol{x}\|$ is the Euclidean norm of $\boldsymbol{x}$. Assuming that the all-zero codeword is BPSK modulated and transmitted over a memoryless AWGN channel, the probability that a certain codeword of binary weight b is chosen at the decoder instead of the transmitted all-zero codeword is [8, Eq. 8.1-49] $P_b = Q\left(\sqrt{2\gamma Rb}\right)$, where γ is the signal to noise ratio (SNR) per bit and $R = k/n$. Then a heuristic union lower bound (LB) on the ML error probability (specifically true at high SNRs) is the probability that a codeword of weight d_b is erroneously decoded, $P_{ML} \geq G_{d_b} Q\left(\sqrt{2\gamma R d_b}\right)$. A union upper bound (UB) on the codeword error probability is the sum of all possible errors,

$$P_{ML} \leq \sum_{b \geq d_b} G_b Q\left(\sqrt{2\gamma Rb}\right). \tag{24}$$

Using the average binary weight enumerator for the RS code, the union upper and lower bounds on the error probability could be plotted to estimate the error probability and will be denoted by 'Union ML UB' and 'Union ML LB' respectively. The union bound is loose at low SNRs. Poltyrev described a tangential sphere bound (TSB) on the error probability of binary block codes BPSK modulated in AWGN channels [9]. This is a very tight upper bound on the ML error probability. We use it in conjunction with the average binary weight enumerator to find a tight upper bound on the error probability of ML decoding of RS codes. Divsalar also introduced in [10] a simple tight bound (that involves no integrations) on the error probability of binary block codes, as well as a comparison of other existing bounds.

We evaluate the average performance of RS codes when its binary image is BPSK modulated and transmitted over an AWGN channel. We plotted the (averaged) TSB for ML decoding for the (15,11) and the (31,15) RS codes and compared them with the union upper and lower bounds in figures 4 and 5 respectively. For the (15,11) RS code, the TSB closely upper bounds the actual ML simulation. ML decoding was simulated using the BCJR algorithm on the trellis associated with the binary image of the RS code [19]. It is clear that at low SNRs the (averaged) TSB give a close approximation of the ML error probability. At high SNRs, the TSB coincides with the union UB. The analytic performance of the hard decision Berlekamp-Massey decoder and the HD Guruswami-Sudan list decoder are also shown and denoted by 'HD-BM' and 'HD-GS' respectively. These are in turn compared to the HD ML bound labeled 'HD-ML PSB'. For the $(15, 11)$ code, which is of relatively high rate, over the BPSK AWGN channel, the GS decoder

does not improve over the BM decoder. However, their performance is very close to the averaged HD-ML UB. For the $(31, 15)$ code, the HD-ML UB has more than 2 dB gain over the BM decoder, whereas the GS decoder offers about 0.3 dB coding gain. ML soft decision decoding has about 4 dB gain over BM and 2 dB gain over HD-ML decoding.

5 Conclusion

An averaged binary weight enumerator for RS codes is derived and shown to closely estimate an exact one for a specific basis representation. Bounds on the average binary minimum distance were derived. For high rates, the RS averaged binary image asymptotically satisfies the GV bound. The optimum ML performance of RS codes BPSK modulated over an AWGN channel is analyzed for both soft and hard decision decoding. By comparison with actual simulations for the $(15, 11)$ RS code, the bound based on the TSB is tight. It is useful to compare the performance of existing suboptimum hard and soft decision decoding algorithms with their corresponding ML decoders.

References

[1] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon codes and algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

[2] R. Kötter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.

[3] M. El-Khamy and R. J. McEliece, "Interpolation multiplicity assignment algorithms for algebraic soft-decision decoding of Reed-Solomon codes," to appear in *AMS-DIMACS volume, "Algebraic Coding Theory and Information Theory".*

[4] ——, "Iterative algebraic soft decision decoding of Reed-Solomon codes," in *Proc. of ISITA 2004.*, Parma, Italy, 2004, pp. 1456–1461.

[5] J. Jiang and K. Narayanan, "Iterative soft decision decoding of Reed Solomon codes based on adaptive parity check matrices," in *Proc. ISIT*, 2004.

[6] Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, pp. 384–386, May 1978.

[7] V. Guruswami and A. Vardy, "Maximum likelihood decoding of Reed Solomon codes is NP-hard," submitted to *IEEE Trans. Inform. Theory.*

[8] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.

[9] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.

[10] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," TMO Progress Report, NASA,JPL, Tech. Rep. 42–139, 1999.

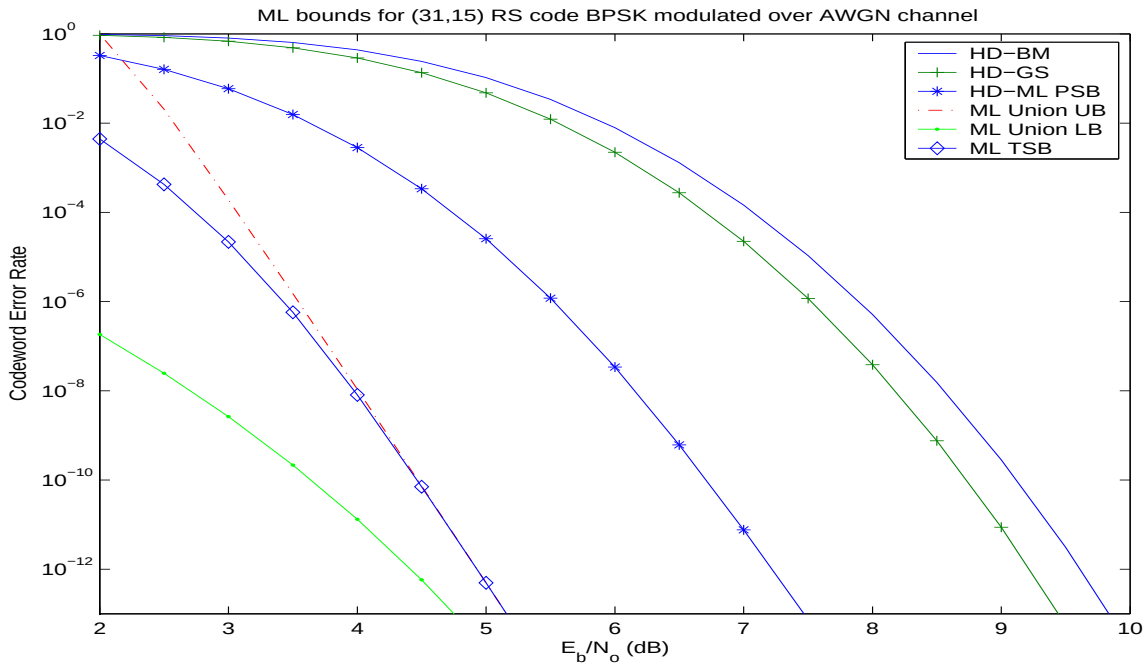

Figure 5: Performance bounds of the $(31, 15)$ RS code, $q = 32$, over AWGN channels.

[11] T. Kasami and S. Lin, "The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed Solomon code over GF(2^m) with generator polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$." *Linear Algebra Appl.*, pp. 291–307, 1988.

[12] I. Blake and K. Kith, "On the complete weight enumerator of Reed-Solomon codes." *SIAM J. Disc. Math.*, vol. 4, no. 2, pp. 164–171, May 1991.

[13] C. Retter, "The average binary weight enumerator for a class of generalized Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 346–349, March 1991.

[14] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge: Cambridge U. Press, 2002.

[15] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge: Cambridge U. Press, 2001.

[16] F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North Holland, 1977.

[17] V. Ponnampalam and B. Vucetic, "Soft decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 50, pp. 1758–1768, Nov. 2002.

[18] R. J. McEliece and L. Swanson, "On the decoder error probability of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 5, pp. 701–703, Sep. 1986.

[19] M. Kan, private Communication.