Tangential sphere bounds on the ensemble performance of ML decoded Gallager codes via their exact ensemble distance spectrum

Sheng Tong

Xidian University, sheng@uow.edu.au
Abstract
An efficient numerical approach to the exact ensemble distance spectrum of Gallager codes has been developed by evaluating powers of polynomials. With the exact ensemble distance spectrum of Gallager codes, tangential sphere upper bounds on their maximum likelihood (ML) decoding performance over binary input AWGN channels are investigated. Numerical results indicate improved bounds have been obtained, better than Sason and Shamai's results (which are based on Gallager's upper bound on the ensemble distance spectrum), especially in the error floor region. Furthermore, some critical properties of Gallager codes, including typical minimum distance and the performance tradeoff in the waterfall and error floor regions, have been considered.

Keywords
exact, their, via, codes, gallager, spectrum, decoded, distance, ml, performance, ensemble, bounds, sphere, tangential

Disciplines
Engineering | Science and Technology Studies

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/eispapers/1108
Tangential Sphere Bounds on the Ensemble Performance of ML Decoded Gallager Codes via Their Exact Ensemble Distance Spectrum

Sheng Tong
Email: ts_xd@163.com

Abstract—An efficient numerical approach to the exact ensemble distance spectrum of Gallager codes has been developed by evaluating powers of polynomials. With the exact ensemble distance spectrum of Gallager codes, tangential sphere upper bounds on their maximum likelihood (ML) decoding performance over binary input AWGN channels are investigated. Numerical results indicate improved bounds have been obtained, better than Sason and Shamai’s results (which are based on Gallager’s upper bound on the ensemble distance spectrum), especially in the error floor region. Furthermore, some critical properties of Gallager codes, including typical minimum distance and the performance tradeoff in the waterfall and error floor regions, have been considered.

I. INTRODUCTION

Low-density parity-check (LDPC) codes were firstly introduced by Gallager in the early of 1960’s [1,2], and rediscovered by MacKay and Neal [3] in the late of 1990’s. In his seminal work, Gallager investigated a special class of regular LDPC codes, referred to as Gallager codes, and provided an analytical upper bound on their ensemble distance spectrum [2], which are further elaborated by Sason and Shamai [7]. Based on Gallager’s ensemble distance spectrum upper bound, Sason and Shamai use tangential sphere bound [4] to investigate the ensemble performance of Gallager codes over binary input AWGN channels under maximum likelihood (ML) decoding [5], which further verifies their capacity-approaching performance at long block lengths.

In this paper, we improve Sason and Shamai’s bounds by using the exact ensemble distance spectrum of Gallager codes. For this purpose, we develop an efficient approach to the exact ensemble distance spectrum of Gallager codes. With the exact ensemble distance spectrum, we use tangential sphere bounding technique to evaluate the ensemble performance of ML decoded Gallager codes over binary input AWGN channels. Tangential sphere bounds are upper bounds and depend on the distance spectrum of the considered code. Although there are several tighter but more involved bounds [11,12], we still employ TSB for its simplicity.

The rest of the paper is organized as follows: in Section II, we briefly review the definition of Gallager codes and then develop an efficient approach to their exact ensemble distance spectrum. In Section III, improved tangential sphere bounds based on the exact ensemble distance spectrum on the ensemble performance of ML decoded Gallager codes over binary input AWGN channels are presented. Furthermore, some properties of Gallager codes, including typical minimum distance and the performance tradeoff in the error floor regions, are considered. Section IV concludes the paper.

II. CALCULATION OF ENSEMBLE DISTANCE SPECTRUM OF GALLAGER CODES

Following Gallager, an \((n, j, k)\) Gallager code is a length-\(n\) block code, specified by a sparse parity-check matrix \(H\). It is shown in eqn.(1) that the parity-check matrix \(H\) consists of \(j\) sub-matrices \(H^i\) \((i = 1, 2, \cdots, j)\) of the same size, each containing a single 1 in each column and \(k\) 1’s in each row. The first sub-matrix \(H^1\) is constructed in a staircase form, i.e., the \(k\) 1’s in its \(i\)th row are located from the \((i-1)k+1\)th column to the \((ik)\)th column, as shown in eqn.(2). The other sub-matrices are just random permutations of the first one. Every sub-matrix \(H^i\) defines a super code \(C^i\), which can be viewed as the direct sum of \((n/k)\) same single parity-check (SPC) codes, each denoted as \((k, k-1, 2)\). Thus, Gallager code can be interpreted as the intersection of the \(j\) super codes.

\[
H = \begin{pmatrix}
H^1 \\
H^2 \\
\vdots \\
H^j
\end{pmatrix}
\]

(1)

where

\[
H^1 = \begin{pmatrix}
1 & \cdots & 1 \\
k & \cdots & k \\
1 & \cdots & 1
\end{pmatrix}
\]

(2)

Now we consider the ensemble distance spectrum of \((n, j, k)\) Gallager codes. From above, the ensemble distance spectrum of Gallager codes can be obtained via a two-step procedure. We shall first outline the two-step procedure in the following and then discuss the two steps in details.
Calculation of the Ensemble Distance Spectrum of 
\((n, j, k)\) Gallager Codes

1) Calculate the distance spectrum of each super code. 
Note that the other \((j-1)\) super codes are just random permutations of the first one. We only need to find the distance spectrum for the first super code \(C^1\).

2) Under the uniform interleaver assumption, the distance spectrum of Gallager codes can be easily derived from those of the super codes.

Firstly, the step 1) is considered. For a code \(C\) of length-\(n\), denote its weight enumerating function (WEF) as

\[ A^C(X) = \sum_{d=0}^{n} A_d X^d, \]  

where \(A_d\) is the number of codewords of weight-\(d\). From eqn.(2) and the fact that the super code \(C^1\) is the direct sum of \(n/k\) \((k,k-1,2)\) SPC codes, the WEF of \(C^1\) can be obtained from that of a \((k,k-1,2)\) SPC code as follows.

\[ A^{C^1}(X) = [A^{SPC}(X)]^{[n/k]}, \]  

where \(A^{SPC}(X)\) denotes the WEF of a \((k,k-1,2)\) SPC code, given by

\[ A^{SPC}(X) = \sum_{i=0}^{[k/2]} \binom{k}{2i} X^{2i}, \]  

where \([x]\) denotes the largest integer not greater than \(x\).

From eqn.(4), it is known that the calculation of the distance spectrum of \(C^1\) only involves a power of a polynomial \(A^{SPC}(X)\), which contains a relatively small number of terms for \(k\) not greater than a few dozens. It is known that polynomial multiplication can be interpreted as vector convolution, which can be efficiently done using FFT\(^1\). However, due to the numerical problems in the calculation, this approach does not work well even for a block length of a few hundreds of bits.

Fortunately, there have been developed several efficient methods for evaluating powers in [9]. For simplicity, we use the “right-to-left binary method” to evaluate eqn.(4). For example, to evaluate \(f(x)^{23}\), we first write the index 23 in its binary representation, i.e., 10111. Then replace each “1” by the pair of letters “SX”, replace each “0” by “S”, and delete the “SX” at the most left side. The obtained sequence is “SSXSXSXS”, which gives the rule for computing \(f(x)^{23}\) by interpreting each “S” as squaring and each “X” as multiplying by \(f(x)\). More clearly, we should successively compute \(f(x)^2, f(x)^4, f(x)^5, f(x)^{10}, f(x)^{11}, f(x)^{22}, f(x)^{23}\). Generally, to evaluate \(f(x)^m\) for a positive integer \(m\), the required number of polynomial multiplications by the right-to-left binary method is \([\log_2(m)] + v(m) - 1\), where \(v(m)\) denotes the number of “1”s in the binary representation of \(m\). Thus, to evaluate eqn.(4), we should carry out \([\log_2(n/k)] + v(n/k) - 1\) times of polynomial multiplications.

\(^1\)Note that the vector convolution used here is linear convolution. To avoid circular convolution, we must pad zero terms to \(A^{SPC}(X)\) to the term of \(X^n\) before applying an FFT.

Once we get the WEF for the first super codes, we also get WEF’s for the other super codes since they are just random permutations of the first super code. Thus, all super codes share the same WEF.

Now, we consider the step2). Under the uniform interleaver assumption, the probability of a weight-\(d\) codeword of \(C^1\) being a codeword of another super code is \(A^C_d / \binom{n}{d}\). Thus, the average number of weight-\(d\) codewords in an \((n, j, k)\) Gallager code \(C\) is

\[ A^C_d = \frac{A^{C^1}_d}{\binom{n}{d}} j, k. \]  

Obviously, eqn.(6) gives the \(d\)-th term of the ensemble distance spectrum \(A^C\) for \((n, j, k)\) Gallager codes. Thus, we obtain the ensemble distance spectrum for Gallager codes.

III. NUMERICAL RESULTS

In his seminal work [2], Gallager also derived an upper bound on the ensemble distance spectrum of Gallager codes. The comparison between the exact ensemble distance spectrum and Gallager’s upper bound on ensemble distance spectrum of Gallager codes is presented in Fig.1, for some \((n,3,6)\) Gallager code ensembles with \(n = 108, 504, 1008, 10008\). As already indicated in [4], the shaping of the distance spectrum of these ensembles of Gallager codes is rather typical for other block lengths and rates. Fig.1 shows that with the increase of code lengths Gallager’s upper bounds get closer to the exact ensemble distance spectrum. It is seen from Fig.1 that Gallager’s upper bound just lays above the exact ensemble distance spectrum of \((10008,3,6)\) Gallager codes. Hence, for long block lengths, performance in the waterfall region estimated via Gallager’s distance spectrum upper bound become very close to those obtained from the exact distance spectrum by using the tangential sphere bounding technique, as shown in Fig.3(b). However, there is still a observable difference at the low weight part, which determines a significant performance difference in the error floor region, which is also indicated in Fig.3(b).

Gallager also proved that for every pair of \((j, k)\) with \(j \geq 3\), there is a normalized Hamming threshold weight such that for Hamming weight below it, the exponent of the upper bound on the ensemble distance spectrum is negative [2]. Thus, for large block lengths, the typical minimum distance increases linearly with block length for \((n, j, k)\) Gallager codes. In this paper, with the exact ensemble distance spectrum \(A^C\) of \((n, j, k)\) Gallager codes, we define their typical minimum distance as the minimum positive integer \(d\) such that \(A^C_d \geq 1\), i.e.,

\[ d^*_\text{min} = \min\{d|d > 0, A^C_d \geq 1\} \]  

Typical minimum distance of Gallager codes for different pairs of \((j, k)\) and block lengths are shown in Fig.2. From Fig.2, it is seen that for a fixed pair of \((j, k)\), the typical minimum distance grows almost linearly with the block length. Moreover, for a fixed ratio of \(j/k\) (i.e., keeping the code rate constant) and a fixed block length \(n\), increasing the values of \(j\) and \(k\) will effectively increase the typical minimum distance.
TABLE I
NORMALIZED TYPICAL MINIMUM DISTANCE FOR GALLAGER CODES.

<table>
<thead>
<tr>
<th>(j, k)</th>
<th>(3,6)</th>
<th>(4,8)</th>
<th>(5,10)</th>
<th>(6,12)</th>
<th>(10,20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>δ_{j,k}</td>
<td>0.0235</td>
<td>0.0633</td>
<td>0.0847</td>
<td>0.0958</td>
<td>0.1082</td>
</tr>
</tbody>
</table>

These numerical results agree well with Gallager’s analytical analysis. The ratios δ_{j,k} of typical minimum distance to block length for given pairs of (j, k) are listed in Table I. These δ_{j,k}’s are obtained by curve fitting using the least square method with the data provided in Fig.2, which can be interpreted as the normalized typical minimum distance with respect to the block length.

Tangential sphere upper bounds on the ML decoding performance of some ensembles of (n, j, k) Gallager codes with rate-0.5 are presented in Fig.3(a) and (b). Fig.3(a) shows that tangential sphere bounds via exact ensemble distance spectrum improve greatly over those based on Gallager’s upper bound on ensemble distance spectrum in both the waterfall region and the error floor region for medium block lengths. By comparing Fig.3(a) and (b), we see that with the increase of block length, the improvement in the waterfall region decreases, while there is still a significant improvement in the error floor region. It is also seen from Fig.3(a) and (b) that for a fixed block length and ratio of j/k, the performance of Gallager codes improves with the increase of j and k. Moreover, Fig.3(a) and (b) also demonstrate the effect of block length on the performance of Gallager codes for a fixed pair of (j, k). For example, for the case of j = 6 and k = 12, the values of Eb/N0 in decibel required by tangential sphere bounds on block error rate via
exceptional performance. Note that the true rate of
are summarized in Table II, demonstrating their potential
rate of $10^{-5}$, respectively. For Gallager codes to achieve a block error
and a fixed ratio of $10^{-5}$, (10008, 6, 12) Gallager codes beat slightly (10008, 12, 24)
which contributes a lot to the waterfall region performance. Thus, (10008, 12, 24)
Gallager in the waterfall region.

IV. CONCLUSIONS

By developing an efficient approach to ensemble distance spectrum of Gallager codes, we have investigated the ensemble performance of ML decoded Gallager codes over binary input AWGN channels using the tangential sphere bounding technique. Our conclusions are summarized as follows:

1) With the increase of block lengths, the difference between Gallager’s upper bound on ensemble distance spectrum and the exact distance spectrum of Gallager codes decreases. However, it is still observable in the low weight part, which determines that there remains a significant performance difference in the error floor region, as evidenced in Fig.3(b).

2) For Gallager code ensembles with a fixed pair of $(j, k)$, their typical minimum distance grows almost linearly with block lengths, which agrees well with Gallager’s analytical results based on his upper bound on distance spectrum.

3) For a fixed ratio of $j/k$, by increasing the column weight $j$ to a relatively large value (say a few dozens), a performance tradeoff between the waterfall region and error floor region can be observed (see Fig.4(b)).

4) ML performance evaluation of Gallager codes using the tangential sphere bounds shows that increasing the column weight $j$ for a fixed ratio of $j/k$ and a constant block length will greatly improve the performance of Gallager codes, especially in the error floor region. However, for suboptimal and practical iterative decoders, the density evolution analysis [8] shows that for regular LDPC codes the column weight of $j = 3$ works the best. A promising solution to this dilemma of binary Gallager codes is non-binary codes. More clearly, in the binary representation of the parity check matrix of an LDPC code over $GF(q)$, every non-binary element in the parity check matrix can be replaced by a small binary
TABLE II
VALUE OF $E_b/N_0$ REQUIRED FOR TANGENTIAL SPHERE UPPER BOUND ON BLOCK ERROR RATE OF $10^{-5}$ WITH ML DECODING FOR $(n, j, k)$ GALLAGER CODE ENSEMBLE WITH $j = 6$ (ASSUMING BPSK MODULATION AND AWGN CHANNELS). BOTH VALUE OF $E_b/N_0$ VIA EXACT ENSEMBLE DISTANCE SPECTRUM (LISTED BEFORE VIRGULES) AND THOSE VIA DISTANCE SPECTRUM UPPER BOUND (LISTED AFTER VIRGULES) ARE GIVEN.

<table>
<thead>
<tr>
<th>The number of ones ($k$) in each row of the parity matrix $H$ of the code ensemble and design code rate (R) (Shannon limit)</th>
<th>$k = 8$</th>
<th>$k = 10$</th>
<th>$k = 12$</th>
<th>$k = 18$</th>
<th>$k = 24$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R = 0.250$</td>
<td>$(-0.79dB)$</td>
<td>$(-0.24dB)$</td>
<td>$(0.19dB)$</td>
<td>$(1.06dB)$</td>
<td>$(1.63dB)$</td>
</tr>
<tr>
<td>$R = 0.31dB$</td>
<td>$0.53dB$</td>
<td>$2.17dB$</td>
<td>$1.85dB$</td>
<td>$0.09dB$</td>
<td>$0.1$</td>
</tr>
<tr>
<td>$R = 1.52dB$</td>
<td>$3$</td>
<td>$0.74dB$</td>
<td>$2.39dB$</td>
<td>$0.62dB$</td>
<td>$0.5$</td>
</tr>
<tr>
<td>$R = 2.19dB$</td>
<td>$0.91dB$</td>
<td>$(-1.63dB)$</td>
<td>$0.55dB$</td>
<td>$0.79dB$</td>
<td>$0.35dB$</td>
</tr>
<tr>
<td>$R = 2.57dB$</td>
<td>$0.91dB$</td>
<td>$1.53dB$</td>
<td>$2.19dB$</td>
<td>$(-0.24dB)$</td>
<td>$0.20dB$</td>
</tr>
</tbody>
</table>

Fig. 4. Illustration of the performance tradeoff between the waterfall region and error floor region for two rate-0.5 Gallager code ensembles. a) distance spectrum; b) tangential sphere upper bound on block error rate.

square matrix\(^2\), in which some columns may contain several ones, thus increasing the average column weight, while in the representation of the parity check matrix over GF($q$) the column weight can be still very small and suitable for iterative decoders. This implies we can construct non-binary LDPC codes which perform well for both ML decoder and iterative decoders [10].

REFERENCES


\(^2\)Note that all these binary square matrices and the all zero matrix of the same size form the finite field, GF($q$).