

A New Bound to Error Probability on AWGN Channels: From Folded Coding to Gaussian Random Coding

DENGSHENG LIN (Member, IEEE), AND YUE XIAO^{ID} (Member, IEEE)

National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

CORRESPONDING AUTHOR: Y. XIAO (e-mail: xiaoyue@uestc.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2020YFB1807203.

ABSTRACT A new bound on the error probability of coding with limited code length over additive white Gaussian noise (AWGN) channels is proposed. The developed bound is proved to be universal for two connected encoding ways. On the one hand, we conceive folding the conventional codes, such as Hadamard and binary random ones, in order to adapt shorter code length. On the other hand, we further extend the above folded structure to Gaussian random coding and hence to bound its error probability. Finally, we demonstrate that the bound of the above two constructions can be unified as $\sqrt{\frac{\log_2 e}{2\pi n C}} 2^{-n(C/2-R)}$ where C represents the capacity of the AWGN channel, n and R stand for the code length and rate, respectively. This theoretical contribution confirms that, in the context of short code length and low rate, the developed two constructions exhibit excellent performance even close to the Shannon bound on AWGN channels.

INDEX TERMS AWGN, Hadamard code, binary random code, capacity.

I. INTRODUCTION

THE GREAT progress on channel coding has been made in the recent three decades [1]–[5], toward achieving the capacity with affordable implementation complexity. More explicitly, three kinds of milestone coding techniques, as Turbo code [1], low-density parity-check(LDPC) code [2]–[4] and polar code [5], nowadays have been at the center of attention of the coding community, by offering powerful forward error control (FEC) capability for modern cellular mobile communication systems [6], [7]. Despite the outstanding performance in practical use, current theoretical analysis works such as [5] have proven that the Shannon capacity can be ultimately reached on discrete memoryless channels.

According to the classical coding theorem, the capacity-achieving FEC depends on the increase of the code length [8], due to the fact that in the asymptotic regime, the block error ratio (BLER) can decrease exponentially with the code length. This phenomenon can be described as [8]

$$P_e < 2^{-n(C-R)},$$

where n means code length, C and R stand for the capacity and the rate, respectively. The above theoretical proof is based on the so-called asymptotic equipartition property (AEP) [9]. Meanwhile, Gallager also developed another theoretical proof in [10] resulting in

$$P_e < \exp(-nE(R)),$$

where

$$E(R) = \max_{\rho, p_k} (-\rho R + E_o(\rho, p_k))$$

is termed as error exponent while ρ is a real number between $(0, 1]$. And

$$E_o(\rho, p_k) = -\log \left(\sum_{i=1}^J \left(\sum_{k=1}^K p_k P_{i,k}^{1/(1+\rho)} \right)^{1+\rho} \right),$$

in which p_k represents the probability of input alphabet of K symbols while $P_{i,k}$ denotes the channel transition probability with J output symbols. Therefore, the optimal rate R ($0 \leq R < C$) can be achieved by maximizing $E_o(\rho, p_k)$ over ρ and input probabilities p_k [10].

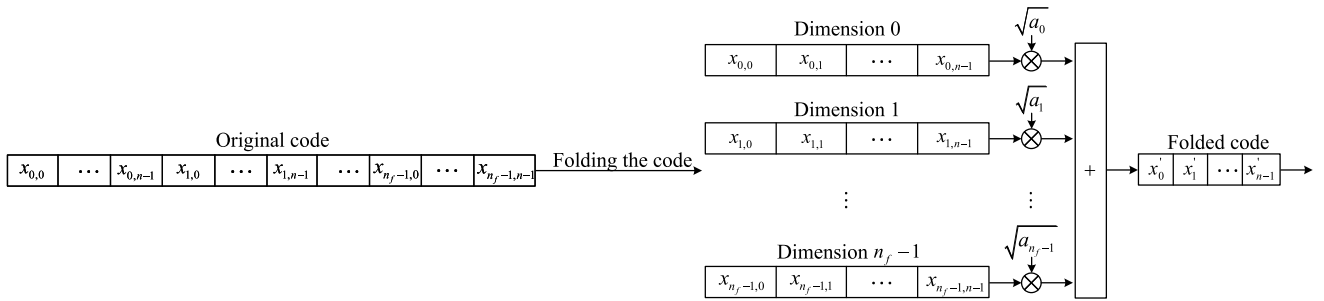


FIGURE 1. Folding the code towards shorter code length.

The above-mentioned theoretical results are attained based on the assumption that the code length is enough large. However, for some recently emerging scenarios such as ultra-reliable low latency communications (URLLC) [11], [12], the code length will be limited to a finite extent in order to shorten the time delay, while the reliability is still expected to remain an ultra high level, such as an error probability of 10^{-5} within 1 millisecond described in [11]. As a result, this scenario will bring double challenges for channel coding. Unfortunately, most of the existing coding techniques [13]–[16] only work well in the middle-reliability region instead of the high-reliability one, which motivates us to focus on this region in the context of limited code length.

Meanwhile, it has become crucial to evaluate the coding performance in the non-asymptotic regime [17]. Although for finite length, there is no exact expression to bridge the coding parameters and the error probability [18], most researches tended to utilize attainable inequalities and approximations to bound the performance of various families of short codes [19]–[23]. Specifically, C. E. Shannon firstly proposed a tight lower bound of error probability over additive white Gaussian noise (AWGN) channels based on packing spherical cones [24]. More sphere-packing bounds for moderate code length were derived in [25] and [26]. Gallager further developed another new bound based on Gaussian random coding [27]. In [18], Polyanskiy *et al.* introduced a series of new lower and upper bounds for finite-length codes on various channels including the binary symmetric channel, binary erasure channel and AWGN channel. Especially, an exact normal approximation was also proposed as a uniform expression for classic channels, written as

$$P_e \approx Q\left(\sqrt{\frac{n}{v}}(C - R)\right)$$

where $Q(\cdot)$ represents the complementary Gaussian cumulative distribution function and v is channel dispersion defined as the variance of information density under the capacity achieving distribution of codewords. In the context of AWGN channel, for example, channel dispersion is given as

$$v = \frac{P(P+2)}{2(P+1)^2} \log_2^2(e),$$

where P denotes the transmit power [18].

Following the above-mentioned current theoretical works, a new upper bound of error probability is developed in this

contribution for coding in AWGN channels, in order to theoretically disclose the high-reliability region under limited code length. Specifically, the bound is obtained by folding the conventional codes such as Hadamard and binary random ones. Furthermore, we extend this structure to Gaussian random coding. Through theoretical derivation, we demonstrate that all the above coding structures considered exhibit a uniform bound of error probability on AWGN channels, which can be briefly expressed in advance as

$$P_e < \sqrt{\frac{\log_2 e}{2\pi n C}} 2^{-n(C/2-R)}.$$

The above theoretical result achieved in this work has the potential to be a new guidance for coding design. On the one hand, the bound indicates that this way of coding can only achieve a half of the capacity of the AWGN channel when the code length n approaches infinity. On the other hand, we can also exhibit that under limited code length and low code rate, this coding mechanism performs excellently owing to its outstanding error exponent, even close to the Shannon's bound [24]. In general, this coding technique is demonstrated to have the potential to adapt URLLC in the context of high interference, such as massive random-access [28].

The remainder of this manuscript is organized as follows. Section II firstly introduces the concept of code folding, while quantifying its capacity on the AWGN channel. According to the disclosed properties of the folding channel, an upper bound of block error probability on AWGN channel is proposed based on folding the Hadamard code. Furthermore, by extending the code folding structure into a general configuration as the binary random code, the theoretical bound is quantified as an identical form in Section III. Furthermore, Section IV extends the above coding way into Gaussian random coding with theoretical analysis. The numerical results are then presented in Section V, while our concluding remarks are provided in Section VI.

II. FOLDING THE HADAMARD CODE

A. THE WAY OF CODE FOLDING AND ITS CAPACITY

In order to reduce the code length while maintaining the amount of information bits, we firstly consider folding a conventional code as described in Fig. 1. In general, the original code is described as $[x_{0,0}, x_{0,1}, \dots, x_{0,n-1}; x_{1,0}, x_{1,1}, \dots, x_{1,n-1}; x_{n_f-1,0}, x_{n_f-1,1}, \dots, x_{n_f-1,n-1}]$ with length

n_s , whose symbols $x_{i,j}, i = 0, 1, \dots, n_f - 1, j = 0, 1, \dots, n - 1$, are real numbers while obeying standard normal distribution. Then the original code is folded into n_f dimensions where the i th dimension with length n is described as $x_{i,j}, j = 0, 1, \dots, n - 1$. Apparently, the code length is reduced from n_s to $n = n_s/n_f$ by folding the original code into the ultimate super-symbols as

$$x'_j = \sum_{i=0}^{n_f-1} \sqrt{a_i} x_{i,j}, \quad (1)$$

where a_i stands for the power scaler of each dimension. Then the folded super-symbols are transmitted through the AWGN channel as

$$y_j = x'_j + z_j, \quad (2)$$

where z_j is the noise term with standard normal distribution.

We substitute Eq. (1) into Eq. (2) and let

$$x'_{i-1,j} = \sum_{t=0}^{i-1} \sqrt{a_t} x_{t,j}, \quad (3)$$

$$x''_{i+1,j} = \sum_{t=i+1}^{n_f-1} \sqrt{a_t} x_{t,j} \quad (4)$$

and

$$y_{i,j} = y_j - x'_{i-1,j} \quad (5)$$

for $i > 0$. Then Eq. (2) can be rewritten as

$$y_{i,j} = \sqrt{a_i} x_{i,j} + x''_{i+1,j} + z_j. \quad (6)$$

Suppose that the decoder can perfectly recover $x'_{i-1,j}$ step by step, so $y_{i,j}$ can be correctly achieved. In this case, the interference to $x_{i,j}$ is determined by $x''_{i+1,j}$. We further define the i th sub-channel as

$$y_{i,j} = \sqrt{a_i} x_{i,j} + z_{i,j}, \quad (7)$$

where

$$z_{i,j} = x''_{i+1,j} + z_j. \quad (8)$$

Clearly, the i th sub-channel is also an AWGN channel with mean 0 and variance

$$\sigma_i^2 = \begin{cases} \sum_{t=i+1}^{n_f-1} a_t + 1, & i < n_f - 1 \\ 1, & i = n_f - 1. \end{cases} \quad (9)$$

So the SNR of the i th sub-channel is expressed as

$$S_i = \frac{a_i}{\sigma_i^2}. \quad (10)$$

To keep the SNR of each sub-channel as a constant S_f , combining Eq. (9) and Eq. (10), we arrive at

$$a_i = S_f (S_f + 1)^i. \quad (11)$$

We demonstrate that there exists a power scaler a_i for each sub-channel to keep a constant SNR. Thus, the transmit super-symbol x'_j is with power

$$a = \sum_{i=0}^{n_f-1} a_i = (S_f + 1)^{n_f} - 1. \quad (12)$$

The capacity of the AWGN channel with SNR $S = a$ is then expressed as

$$C = \frac{1}{2} \log_2(1 + S). \quad (13)$$

On the other hand, following (12), we have

$$\log_2(1 + S) = n_f \log_2(1 + S_f), \quad (14)$$

i.e.,

$$C = n_f C_f, \quad (15)$$

where

$$C_f = \frac{1}{2} \log_2(1 + S_f) \quad (16)$$

is the capacity of the sub-channel. The above result shows that the way of code folding will not reduce the capacity of the AWGN channel.

B. FOLDING THE HADAMARD CODE

Following the above-mentioned structure, we tend to fold conventional Hadamard code as an example. At the beginning, an $n_s \times n_s$ Hadamard matrix can be recursively constructed as [29]

$$H_{n_s} = \begin{bmatrix} H_{n_s/2} & H_{n_s/2} \\ H_{n_s/2} & -H_{n_s/2} \end{bmatrix}. \quad (17)$$

Let $H_1 = 1$, while considering all of the row vectors in H_{n_s} as the codewords, then the matrix can carry $k = \log_2 n_s$ information bits. Based on the properties of Hadamard code, the inner product of any pair of row vectors will be zero [30]. In other words, their Euclidean distance d is equal to $\sqrt{2n_s}$. Note that, since Hadamard code is a kind of binary code, it doesn't strictly satisfy the condition of Gaussian folded noise introduced in Section II-A. However, in the following Section IV-A, we will theoretically demonstrate that the folded Hadamard code can approach Gaussian distribution when n_f goes to infinity.

Based on the union bound, the block error rate of the code in the AWGN channel with SNR S_f can be described as [31]

$$P_e \leq 2^k Q\left(\sqrt{\frac{n_s}{2} S_f}\right), \quad (18)$$

where

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) dt. \quad (19)$$

Note that, the Hadamard code is now expected to be now transmitted in the folded Gaussian channel, according to the process of Fig. 1. Then the symbols from different dimensions n_f are overlapped to generate the transmit symbol $x'_j, j = 0, 1, \dots, n - 1$. Consequently, the folded code is with length n and rate $R = k/n$. Following the definition of the folded channel, there are n_f AWGN sub-channels with constant SNR S_f . So Eq. (18) holds for the folded channel.

By substituting Eq. (14) into Eq. (18), we have

$$P_e \leq 2^k Q\left(\sqrt{\frac{1}{2} n n_f ((S+1)^{1/n_f} - 1)}\right). \quad (20)$$

Then, the following limit holds as

$$\begin{aligned} \lim_{n_f \rightarrow \infty} n_f \left((S+1)^{1/n_f} - 1 \right) \\ = \log(S+1) \\ = \frac{2C}{\log_2 e}. \end{aligned} \quad (21)$$

Therefore, when $n_f \rightarrow \infty$, substituting Eq. (21) into Eq. (20), we have

$$P_e \leq 2^k Q\left(\sqrt{\frac{nC}{\log_2 e}}\right). \quad (22)$$

Furthermore, considering [32]

$$Q(x) < \frac{1}{\sqrt{2\pi}x} \exp\left(-\frac{x^2}{2}\right), \quad (23)$$

we finally arrive at

$$P_e < \sqrt{\frac{\log_2 e}{2\pi nC}} 2^{-n(C/2-R)}. \quad (24)$$

The above result exhibits that the block error probability of the folded Hadamard code is exponentially descending with the code length only if the rate is less than $C/2$. Clearly, the bound cannot achieve the Shannon capacity which requires R asymptotically close to C along with the code length. However, in the context of low code rate and short code length, the bound exhibits excellent good performance owing to its excellent error exponent.

At the receiver, to achieve the bound, a successive interference cancellation algorithm is assumed to perfectly recover the symbols from the sub-channels step by step. Otherwise, the performance will decrease. Moreover, the complexity of decoding is a function of n_s , which is normally much larger than the code length n . In Section IV, we will demonstrate that the proposed code is actually equivalent to Gaussian random code. In this case, the complexity of decoding will decrease to be a function of n .

III. FOLDING THE BINARY RANDOM CODE

For the Hadamard code, n_s is always equal to 2^k . It implies that the information length k will go to infinity along with $n_f \rightarrow \infty$. So the bound shown in Eq. (24) only holds for infinite information length. In the following, we will demonstrate that Eq. (24) still holds even if we break through the

original limitation of the equivalent distance property of the Hadamard code, so as to develop a general way of folding the binary random code. Since there is no fixed relation between k and n_s for the binary random code, it allows the existence of finite k with infinite n_s and n_f . As a result, the bound will be extended to the configuration of arbitrary code rate and code length.

By uniformly selecting 2^k binary sequences with length n_s , the Hamming distance between any two sequences will obey binomial distribution with mean $n_s/2$ and variance $n_s/4$. Meanwhile, it will converge to normal distribution with n_s going to infinity based on De Moivre-Laplace theorem [33]. In other words, the squared Euclidean distance between any two sequences obeys normal distribution with mean $n_s/2$ and variance $n_s/4$. Then the probability density function (PDF) of the Euclidean distance can be written as

$$P_d(x) = \begin{cases} \frac{\sqrt{2x}}{\sqrt{\pi\sigma_s^2}} \exp\left(-\frac{(x^2-\mu_s)^2}{2\sigma_s^2}\right), & x \geq 0 \\ 0, & x < 0, \end{cases} \quad (25)$$

where $\mu_s = n_s/2, \sigma_s^2 = n_s/4$. Therefore, the BLER can be further expressed as

$$P_e = 2^k P_{e1}, \quad (26)$$

where

$$P_{e1} = \int_0^\infty P_d(x) Q(\sqrt{S_f}x) dx. \quad (27)$$

The integral in Eq. (27) cannot be obtained directly. Therefore, we define $\lambda \in (0, 1)$ and split the above integral into two terms as

$$\begin{aligned} P_{e1} = \int_0^{\lambda\sqrt{n_s/2}} P_d(x) Q(\sqrt{S_f}x) dx \\ + \int_{\lambda\sqrt{n_s/2}}^\infty P_d(x) Q(\sqrt{S_f}x) dx, \end{aligned} \quad (28)$$

where $Q(x)$ is a monotonous decreasing function with $Q(x) \leq 1/2$, and

$$\int_0^\infty P_d(x) dx = 1. \quad (29)$$

Then, we arrive at

$$\begin{aligned} P_{e1} &\leq \frac{1}{2} \int_0^{\lambda\sqrt{n_s/2}} P_d(x) dx + Q\left(\lambda\sqrt{\frac{1}{2}S_f n_s}\right) \int_{\lambda\sqrt{n_s/2}}^\infty P_d(x) dx \\ &\leq \frac{\theta}{2} + Q\left(\lambda\sqrt{\frac{1}{2}S_f n_s}\right), \end{aligned} \quad (30)$$

where

$$\theta = \int_0^{\lambda\sqrt{n_s/2}} P_d(x) dx. \quad (31)$$

Based on Chebyshev inequality [33], i.e.,

$$P_d(|x - E| > \epsilon) < \frac{V}{\epsilon^2}, \quad (32)$$

where E and V denote the mean and variance of $P_d(x)$, respectively, in the context of

$$\epsilon = E - \lambda \sqrt{\frac{n}{2}}, \quad (33)$$

we have

$$\begin{aligned} \theta &= P_d\left(x < \lambda \sqrt{\frac{n_s}{2}}\right) \\ &< \frac{V}{\left(E - \lambda \sqrt{\frac{n_s}{2}}\right)^2}. \end{aligned} \quad (34)$$

Since $P_d(x)$ cannot be directly achieved, we tend to derive its upper and lower bound in order to further simplify Eq. (30). Considering that $P_d(x^2)$ obeys normal distribution with mean $E(x^2) = n_s/2$, in the following, we aim at achieving a lower bound of E . According to the former definition, we have

$$\begin{aligned} E &= \int_0^{+\infty} x P_d(x) dx \\ &= \int_0^{+\infty} x \frac{\sqrt{2x}}{\sqrt{\pi n_s/4}} \exp\left(-\frac{(x^2 - n_s/2)^2}{n_s/2}\right) dx. \end{aligned} \quad (35)$$

Then Eq. (35) can be rewritten as

$$E = \int_0^{+\infty} \frac{(n_s/2)^{1/4} \sqrt{x}}{\sqrt{\pi}} \exp\left(-\left(x - \sqrt{\frac{n_s}{2}}\right)^2\right) dx. \quad (36)$$

Let $\alpha = (n_s/2)^{1/2}$ and $\beta = (n_s/2)^{1/4}$ with $\alpha - \beta > 0$, then we have

$$\begin{aligned} E &> \int_{\alpha-\beta}^{\alpha+\beta} \frac{\beta \sqrt{x}}{\sqrt{\pi}} \exp\left(-(x - \alpha)^2\right) dx \\ &> \int_{\alpha-\beta}^{\alpha+\beta} \frac{\beta \sqrt{\alpha - \beta}}{\sqrt{\pi}} \exp\left(-(x - \alpha)^2\right) dx \\ &= \frac{\sqrt{n_s/2 - (n_s/2)^{3/4}}}{\sqrt{\pi}} \int_{-\beta}^{\beta} \exp\left(-x^2\right) dx. \end{aligned} \quad (37)$$

Since

$$\lim_{\beta \rightarrow \infty} \int_{-\beta}^{\beta} \exp\left(-x^2\right) dx = \sqrt{\pi}, \quad (38)$$

we finally arrive at

$$E > \sqrt{n_s/2 - (n_s/2)^{3/4}}. \quad (39)$$

Therefore, an upper bound of the variance can be ultimately obtained as

$$\begin{aligned} V &= E(x^2) - E(x)^2 \\ &< \frac{n_s}{2} - \left(\frac{n_s}{2} - \left(\frac{n_s}{2}\right)^{3/4}\right) \\ &= \left(\frac{n_s}{2}\right)^{3/4}. \end{aligned} \quad (40)$$

Substituting the bounds of E and V into Eq. (34), we have

$$\begin{aligned} \theta &< \frac{\left(\frac{n_s}{2}\right)^{3/4}}{\left(\sqrt{\frac{n_s}{2}} - \left(\frac{n_s}{2}\right)^{3/4} - \lambda \sqrt{\frac{n_s}{2}}\right)^2} \\ &= \frac{1}{\beta \left(\sqrt{1 - \frac{1}{\beta}} - \lambda\right)^2}. \end{aligned} \quad (41)$$

Therefore, there always exists λ infinitely close to 1 when $\beta \rightarrow \infty$ and $\theta \rightarrow 0$. Consequently, Eq. (30) is reduced to

$$P_{e1} \leq Q\left(\sqrt{\frac{1}{2} S_f n_s}\right). \quad (42)$$

Substituting Eq. (42) into Eq. (26) while combining Eq. (18) and Eq. (26), we finally conclude that the BLER bound of the folded binary random coding is identical to that of the folded Hadamard coding as attained in Eq. (24).

Different from the Hadamard code with fixed $n_s = 2^k$, the binary random code is capable of adapting arbitrary code length and rate. So the bound of Eq. (24) holds for a general configuration of finite code length and rate.

IV. FROM BINARY RANDOM CODING TO GAUSSIAN RANDOM CODING

A limitation of the above theoretical work lies in that, binary codes including the Hadamard code and binary random one don't strictly satisfy the condition of Gaussian folded noise introduced in Section II-A. Therefore, we will theoretically demonstrate that the folded binary code can approach Gaussian distribution for each sub-channel defined in Section II-A when n_f goes to infinity.

On the other hand, in order to achieve the bound, the folding number n_f will go to infinity even for finite information length k so that it is unacceptable for practical implementation. In this section, we will further exhibit that the proposed way of folding the codes is actually equivalent to the format of Gaussian random codes. Then, we will also disclose that the bound shown in Eq. (24) still holds when the coded super-symbol x'_j is replaced directly by a Gaussian variable with mean 0 and variance a . Without the folding operation in Eq. (1), the complexity of the encoding and the decoding is only related to k and n rather than n_s and n_f .

A. GAUSSIAN APPROACHING FOR BINARY CODES

Note that the binary sequence obeys binomial distribution with equal probability. Since the original Hadamard code cannot be considered as random sequences, we introduce a perfect permutation to eliminate its regular structure in order to approach the binomial distribution. Then the folded super-symbol x'_j is generated following Eq. (1). Note that here we have $x_{i,j} \in \{-1, 1\}$ for binary code. Considering each folded symbol is with constant power coefficients a_i , there are only n_f values for a_i . By substituting Eq. (14) and Eq. (21) into Eq. (11), we arrive at

$$a_i = \frac{2C}{n_f \log_2 e} (1 + S)^{\frac{i}{n_f}}. \quad (43)$$

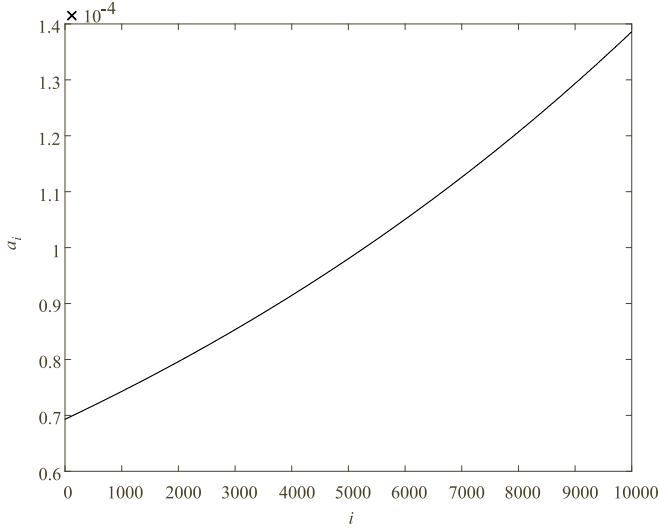


FIGURE 2. An example of a_i with $n_f = 10000$, $a = 1$.

An example of the values of a_i with $n_f = 10000$, $a = 1$ is portrayed in Fig. 2. Note that a_i is monotonously increasing with i . We divide the curve of a_i into $\sqrt{n_f}$ segments, each with length $\sqrt{n_f}$. For convenience, without loss of generality, $\sqrt{n_f}$ is assumed to be an integer. So the beginning and the end of the τ th segment have the values of

$$a_{\tau,1} = \frac{2C}{n_f \log_2 e} (1+S) \frac{\sqrt{n_f}^\tau}{n_f}, \quad 0 \leq \tau < \sqrt{n_f}, \quad (44)$$

and

$$a_{\tau,2} = \frac{2C}{n_f \log_2 e} (1+S) \frac{\sqrt{n_f}^{(\tau+1)-1}}{n_f}. \quad (45)$$

Their ratio is then expressed as

$$\eta_\tau = \frac{a_{\tau,2}}{a_{\tau,1}} = (1+S) \frac{\sqrt{n_f}-1}{n_f}. \quad (46)$$

When $n_f \rightarrow \infty$, we have $\eta_\tau \rightarrow 1$, i.e., $a_{\tau,2} \rightarrow a_{\tau,1}$. Consequently, Eq. (1) is rewritten as

$$x'_j = \sum_{\tau=0}^{\sqrt{n_f}-1} \sqrt{a_{\tau,1}} \omega_{\tau,j}, \quad (47)$$

where

$$\omega_{\tau,j} = \sum_{t=0}^{\sqrt{n_f}-1} x_{\sqrt{n_f}\tau+t,j}. \quad (48)$$

Therefore, when $\sqrt{n_f}$ goes to infinity, $\omega_{\tau,j}$, as the summary of the random variables with binomial distribution, obeys normal distribution with mean zero and variance $\sqrt{n_f}$. Furthermore, since the linear combination of variables with normal distribution also obeys normal distribution, x'_j stands for a Gaussian variable, too. Moreover, although the interference within the same segment doesn't strictly obey Gaussian distribution, the fraction term will gradually approach 0 with the infinite increase of $\sqrt{n_f}$. Considering

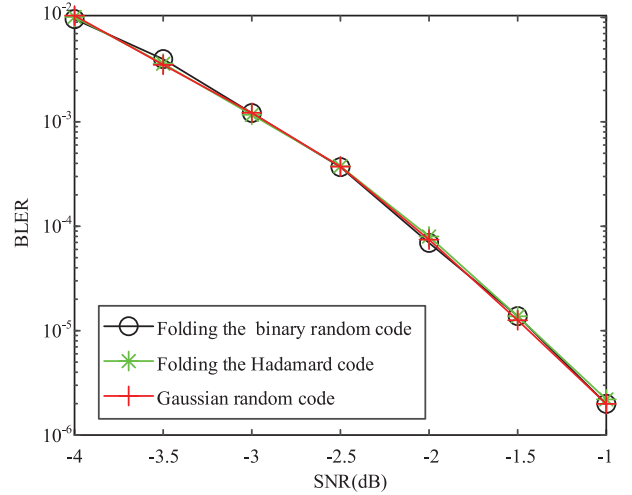


FIGURE 3. Performance comparison of three codes with code length 128 and rate 0.125 based on Hadamard coding, binary random coding, and Gaussian random coding.

$\sqrt{n_f}$ as the number of sub-channel defined in Section II-A and the original code as $\omega_{\tau,j}$, the result in Section II-A is still available for the way of binary coding.

B. FROM BINARY RANDOM CODING TO GAUSSIAN RANDOM CODING

In the previous subsection, we have proven that the coded super-symbols x'_j obey i.i.d. Gaussian distributions with n_f approaching to infinity when they are constructed by folding the binary random code. In the following, we will show that, for any given Gaussian coded super-symbol x'_j , there always exists a binary random sequence with length n_f satisfying Eq. (1), while obeying binomial distribution along with the length n_f going to infinity.

Based on the result in the previous subsection, calculation of Eq. (1) can be divided into two steps by following Eq. (47) and Eq. (48), respectively. For the first step, Eq. (47) can be rewritten as

$$\hat{\omega}_{0,j} = \frac{1}{\sqrt{a_{0,1}}} \left(x'_j - \sum_{\tau=1}^{\sqrt{n_f}-1} \sqrt{a_{\tau,1}} \hat{\omega}_{\tau,j} \right). \quad (49)$$

Following Eq. (49), we firstly randomly generate $\hat{\omega}_{\tau,j}$, $\tau = 1, 2, \dots, \sqrt{n_f}-1$ with standard normal distribution. Then the variable $\hat{\omega}_{0,j}$ can be determined based on Eq. (49). Clearly, $\hat{\omega}_{0,j}$ obeys standard normal distribution, too. Note that $\hat{\omega}_{\tau,j}$, which are considered as real Gaussian variables, are slightly different from $\omega_{\tau,j}$ defined in Eq. (48). But this difference can be negligible according to De Moivre-Laplace theorem [33].

For the second step, Eq. (48) can be written as

$$\omega_{\tau,j} = \omega'_{\tau,j} - \omega''_{\tau,j}, \quad (50)$$

where

$$\omega'_{\tau,j} = \sum_{x_{\sqrt{n_f}\tau+t,j}=1} 1, \quad (51)$$

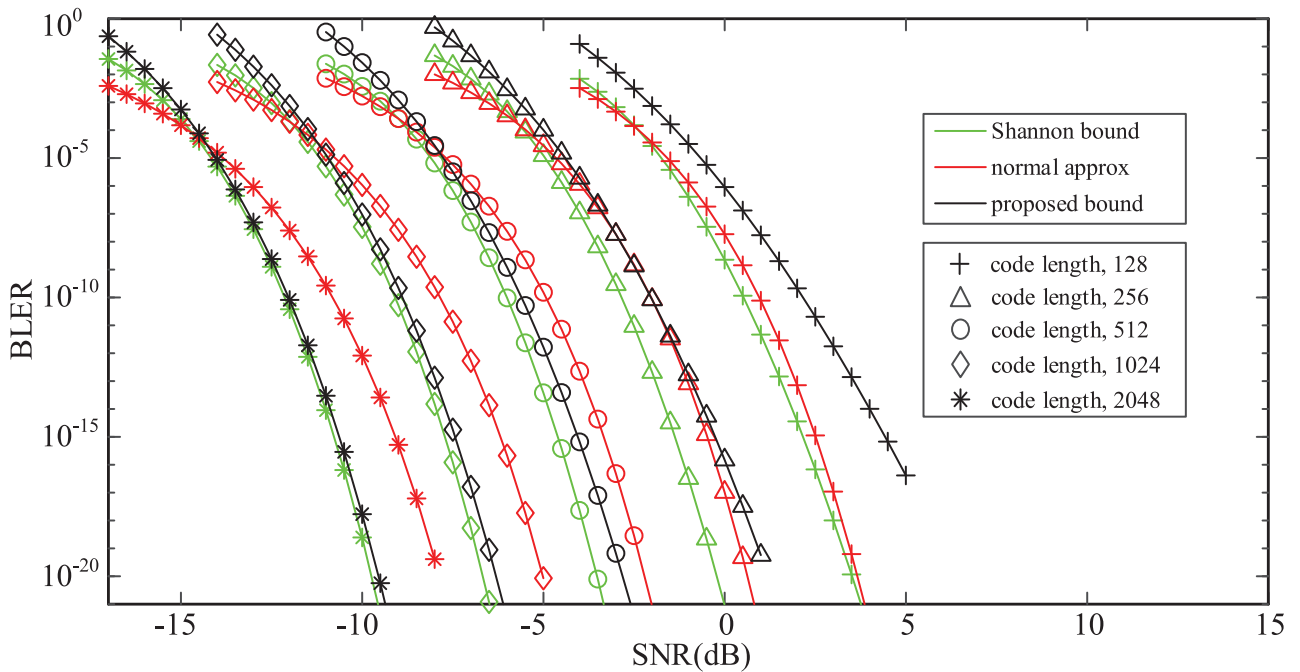


FIGURE 4. The performance of the proposed bound in AWGN channels with extremely high reliability.

and

$$\begin{aligned} \omega''_{\tau,j} &= \sum_{x_{\sqrt{n_f}\tau+i}=-1} 1 \\ &= \sqrt{n_f} - \omega'_{\tau,j}. \end{aligned} \quad (52)$$

Replacing $\hat{\omega}_{\tau,j}$ by $\omega_{\tau,j}$, we have

$$\omega'_{\tau,j} = \left\lceil \frac{\hat{\omega}_{\tau,j} + \sqrt{n_f}}{2} \right\rceil, \quad (53)$$

where $\lceil \cdot \rceil$ means rounding to the nearest integer. Although $\omega'_{\tau,j}$ from Eq. (53) may be larger than $\sqrt{n_f}$, its probability will approach zero when $\sqrt{n_f} \rightarrow \infty$. Following Eq. (48), we construct a binary sequence with $\omega'_{\tau,j}$ “1”s and $\omega''_{\tau,j}$ “-1”s. Moreover, “1”s and “-1”s are randomly generated in the sequence. In other words, the probability of every position being “1” and “-1” in the sequence is equal and independent. Consequently, this binary random sequence obeys binomial distribution.

Combining the analyses in the previous two subsections, we summarize that the transmit super-symbols x_j can be generated directly by Gaussian random variables or by overlapping binary random sequences with amplified power coefficient a_j given in Eq. (1). Compared with the latter way, the way of Gaussian random coding is with lower encoding and decoding complexity only relative to n .

V. RESULTS

In this section, we firstly simulate three codes constructed by the proposed methods to evaluate their BLER performances. These coding ways are based on the Hadamard

coding, binary random coding and Gaussian random coding, respectively. The three codes are all with a code length of 128 and a code rate of 0.125, while the maximum likelihood decoding is used at the receiver. As results, their BLER curves are shown in Fig. 3. From the results, we demonstrate that all these coding ways exhibit similar error performances, as concluded through above-mentioned theoretical analysis. Fig. 4 presents the numerical results for the proposed bound of BLERs in AWGN channels. Note that the derived theoretical result in Eq. (24) is tight in the region of short code length and low code rate, therefore, we focus on the length of information bits k as 16, while the code length n is selected as 128, 512, 1024 and 2048, respectively. For comparison, we also list the Shannon’s bound [24], and the normal approximation presented by Polyanskis *et al.* [18]. Note that, our developed bound is capable of approaching Shannon bound gradually by increasing the code length, in the context of extremely low error floor. This phenomenon supports that the ways of folding the codes and Gaussian random coding could both be theoretically demonstrated to approach the Shannon bound toward extremely high reliability, in the context of low code rate and limited code length. Therefore, our developed coding ways, from code folding to Gaussian random coding, has the potential to apply the scenario with high reliability and sever interference [28]. Furthermore, in Fig. 5, we simulate the BLER performance of Gaussian random coding as an example with maximum likelihood decoding. As expected, the performance of practical coding is between the derived bound and Shannon bound. Specifically, at a BLER of 10^{-5} , when the code length is 128, the performance of Gaussian random coding is only

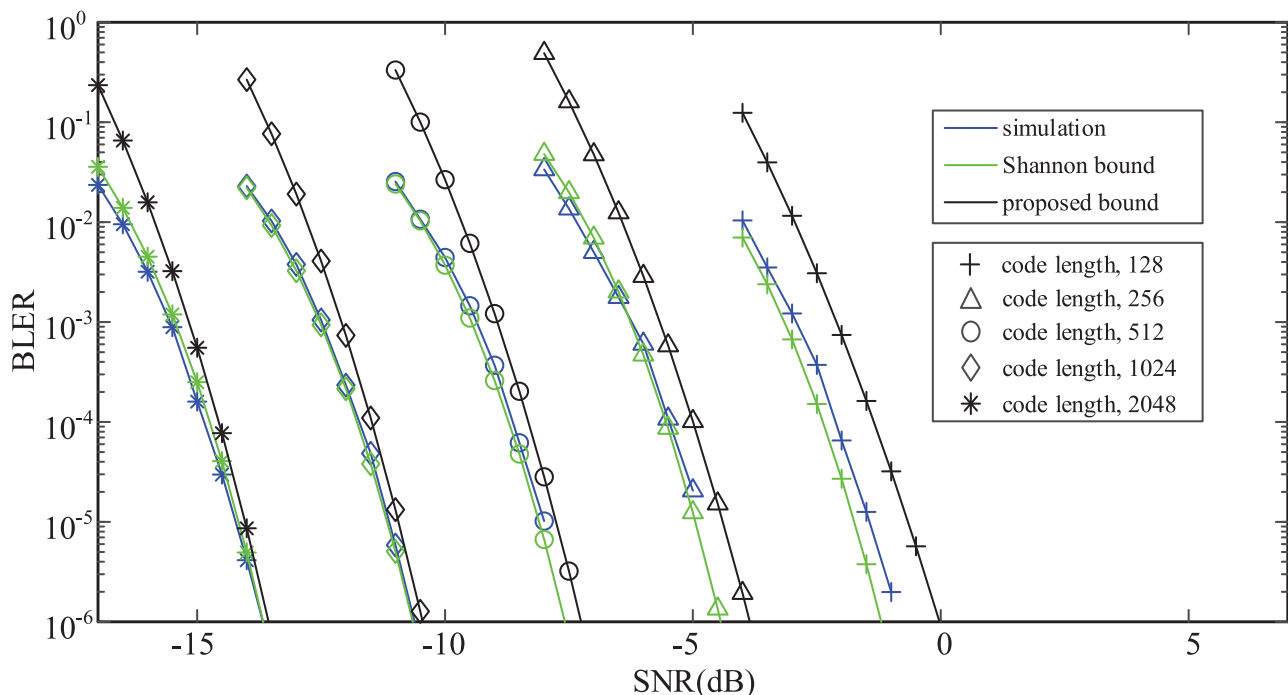


FIGURE 5. The BLER performance of Gaussian random coding through computer simulations.

0.2dB away from the developed bound. As expected, when the code length goes higher, the performance will approach both the derived bound and Shannon bound.

VI. CONCLUSION

Aiming at constructing powerful codes in the context of short code length and low code rate, two connected coding ways as code folding and Gaussian random coding were investigated, by bounding their block error probability performances in the AWGN channel. Through theoretical analysis, we demonstrate that the aforementioned coding ways have a uniform performance bound as $\sqrt{\frac{\log_2 e}{2\pi nC}} 2^{-n(C/2-R)}$, which firstly describes a tradeoff among code length, rate and reliability for code design while demonstrating its advantage in short code length and low rate. Finally, numerical results were also performed to exhibit the excellent performance even close to Shannon bound in the above-mentioned configuration. The above contribution demonstrated that these coding ways have the potential to adapt the scenario of ultra reliability and low latency in the context of massive interference, which will be the focus of our future works.

REFERENCES

- [1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: Turbo-codes. 1," in *Proc. IEEE Int. Conf. Commun.*, May 1993, pp. 1064–1070.
- [2] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.
- [3] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *IEE Electron. Lett.*, vol. 33, pp. 457–458, Mar. 1997.
- [4] S. Y. Chung, G. D. Forney, Jr., T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, Feb. 2001.
- [5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
- [6] *Technical Specification Group Radio Access Network; Multiplexing and Channel Coding (Release 8)*, 3GPP TS Standard 36.212, 2009.
- [7] *Technical Specification Group Radio Access Network; Multiplexing and Channel Coding (Release 16)*, 3GPP Standard TS 38.212, 2020.
- [8] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.
- [9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.
- [10] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. Inf. Theory*, vol. 11, no. 1, pp. 3–18, Jan. 1965.
- [11] "Study on scenarios and requirements for next generation access technologies (release 14)," 3GPP, Sophia Antipolis, France, Rep. TR 38.913, Mar. 2016.
- [12] M. Shirvanimoghaddam *et al.*, "Short block-length codes for ultra-reliable low latency communications," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 130–137, Feb. 2019.
- [13] E. Arikan, "Serially concatenated polar codes," *IEEE Access*, vol. 6, pp. 64549–64555, 2018.
- [14] "Channel coding for URLLC," Huawei, Qingdao, China, 3GPP TSG RAN WG1 NR Ad-Hoc 2, R1-1710004, Jun. 2017.
- [15] "Discussion on channel coding for URLLC channel," 3GPP TSG RAN WG1 NR Ad-hoc Meeting, R1-1700981, Samsung, Spokane, WA, USA, Jan. 2017.
- [16] "Enhanced turbo codes for URLLC," 3GPP TSG RAN WG1 Meeting#87, R1-1702856, AccelerComm, Athens, Greece, Feb. 2017.
- [17] D. Baron, M. A. Khojastepour, and R. G. Baraniuk, "How quickly can we approach channel capacity?" in *Proc. 38th Asilomar Conf. Signals Syst. Comput.*, Nov. 2004, p. 5.
- [18] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

- [19] C. E. Shannon, "Certain results in coding theory for noisy channels," *Inf. Control*, vol. 1, pp. 6–25, Sep. 1957.
- [20] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels I," *Inf. Control*, vol. 10, no. 1, pp. 65–103, 1967.
- [21] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1284–1292, Jul. 1994.
- [22] H. V. Poor and S. Verdu, "A lower bound on the error probability in multihypothesis testing," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1992–1993, Nov. 1995.
- [23] D. E. Lazic, T. Beth, and S. Egner, "Constrained capacity of the AWGN channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, 1998, p. 237.
- [24] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, no. 3, pp. 611–656, May 1959.
- [25] A. Valembois and M. P. C. Fossorier, "Sphere-packing bounds revisited for moderate block lengths," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2998–3014, Dec. 2004.
- [26] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length codes over symmetric memoryless channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1962–1990, May 2008.
- [27] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.
- [28] Y. Polyanskiy, "A perspective on massive random-access," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aug. 2017, pp. 2523–2527.
- [29] W. K. R. Leung, G. Yue, L. Ping, and X. Wang, "Concatenated zigzag hadamard codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1711–1723, Apr. 2006.
- [30] R. Yarlagadda and J. Hershey, *Hadamard Matrix Analysis and Synthesis: With Applications to Communications and Signal/Image Processing*, Boston, MA, USA: Kluwer, 1997.
- [31] S. Lin and D. Costello, *Error Control Coding*. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.
- [32] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. New York, NY, USA: Wiley, 1965.
- [33] W. Feller, *An Introduction to Probability Theory and Its Applications*. New York, NY, USA: Wiley, 1971.



DENGSHENG LIN (Member, IEEE) received the B.E. degree in electronic engineering and the M.S. and Ph.D. degrees in communication and information systems from the University of Electronic Science and Technology of China (UESTC) in 1998, 2004, and 2008, respectively.

He worked as a Research Associate with the Department of Electronic Engineering, City University of Hong Kong in 2005. He was a Visiting Scholar of Communication Theory with the School of Electronic engineering, Royal Institute of Technology, Sweden in 2011. He is currently an Associate Professor with the National Key Laboratory of Science and Technology on Communications, UESTC. His main research interests include channel coding and wireless communications.



YUE XIAO (Member, IEEE) received the Ph.D. degree in communication and information systems from the University of Electronic Science and Technology of China (UESTC) in 2007.

He is currently a Professor with the National Key Laboratory of Science and Technology on Communications, UESTC. He has published more than 100 international journals and has been in charge of more than 20 projects in the area of Chinese 3G/4G/5G wireless communication systems. He is an inventor of more than 50 Chinese and PCT patents on wireless systems. His research interests are in system design and signal processing toward future wireless communication systems. He currently serves as a Senior Associate Editor of IEEE COMMUNICATIONS LETTERS and an Associate Editor of IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY.