Reduced Complexity Ordered Statistics Decoding of Linear Block Codes

Lijia Yang†, Wenhao Chen‡, Li Chen‡
†School of Electronics and Communication Engineering, Sun Yat-sen University, Shenzhen 518107, China
‡School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China
Email:yanglj39@mail2.sysu.edu.cn, chenwh85@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn

2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops) | 978-1-6654-5977-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCWORKSHOPS55477.2022.9896679

***Abstract*—This paper proposes a reduced complexity ordered statistics decoding (OSD) algorithm for linear block codes. With the received information, several most reliable positions in the ordered reliability sequence are prioritized as the validation band (VB). The Gaussian elimination (GE) is then performed to generate the systematic generator matrix of the code. In the process of re-encoding, only the test messages that satisfy the validation rule would be used to generate the codeword candidates, resulting in a low decoding complexity. The decoding error probability upper bound of the proposed OSD is further analyzed to characterize its performance-complexity trade off. Our simulation results show that the proposed OSD can significantly reduce the decoding complexity with a negligible loss in the decoding performance.**

***Index Terms*—linear block codes, maximum-likelihood decoding, ordered statistics decoding, reduced complexity**

I. Introduction

The realization of ultra-reliable low-latency communication (URLLC) requires the support of competent short-to-medium length channel codes. Recent research in short-to-medium length codes [1] has shown that ordered statistics decoding (OSD) of BCH codes can yield a performance that is closed to the finite length transmission limit [2]–[3]. In the OSD, the most reliable independent positions (MRIPs) will first be identified. Then, the test error patterns (TEPs) will be added to the MRIPs of a hard-decision received word to generate codeword candidates. Among all candidates, the most likely one will be selected as the decoding output. Despite its competency in decoding BCH codes, the OSD's exponential complexity remains a practical challenge. In particular, the number of TEPs increases exponentially with the decoding order, resulting in a high decoding complexity. It has also been realized that no information outside the MRIPs is utilized, leaving the decoding capability not fully exploited. In order to reduce the number of TEPs while maintaining the decoding performance, several skipping rules for facilitating the identification of the unpromising TEPs were proposed in [4]–[5]. Meanwhile, stopping rules for identifying the maximum likelihood (ML) codeword from the decoding output list were proposed in [6]–[7], the decoding can be terminated earlier, consequently. Segmentation discard rule was proposed in [8]. By segmenting the TEPs with reasonable boundaries, the frequency of checking the stopping rule can be reduced and the progressive segmented decoding can be realized. In order to use information outside the MRIPs and improve the decoding performance, the box-and-match algorithm (BMA) was proposed in [9]. In the BMA, information outside the MRIPs will first be stored in the memory space. It will then be further utilized to obtain additional performance gains. The iterative information set reduction (IISR) was proposed in [10]. By the iterative update of the most reliable information, decoding performance can be improved. The multiple information sets generated by the randomly biased log-likelihood ratios (LLRs) was proposed in [11], further improving the OSD performance. However, most of the above mentioned approaches introduce the extra decoding complexity either in judging the ML codeword or in utilizing information outside the MRIPs.

The proposed OSD is inspired by the fact that several most reliable positions in the ordered received sequence have an extremely high probability to be error-free. Hence, they can be prioritized as the validation band (VB) for generating the codeword candidates. After determining the length of VB, the Gaussian elimination (GE) will be performed subsequently to obtain the systematic generator matrix. Relatively reliable independent positions (RRIPs) can be determined accordingly. In the re-encoding process, only the test messages that satisfy the validation rule are utilized to generate the codeword candidates and the rest will be discarded. This assessment results in a low decoding complexity. Since the validation process is completed in the re-encoding process, the proposed OSD will not introduce additional decoding complexity and it is also implementation friendly. In order to achieve a better decoding complexity and performance trade off, this paper further characterizes the decoding error probability upper bound of the proposed OSD. Our simulation results will demonstrate the complexity advantage of the proposed complexity reducing OSD.

II. Preliminaries

Let $\mathcal{C}(n,k)$ denote a binary linear block code, where n and k are the length and dimension of the code, respectively. Its generator matrix $\mathbf{G}$ is a $k \times n$ binary matrix written as $\mathbf{G} = [\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n]$, where $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n$ are the column vectors of length k. Let $\underline{\boldsymbol{f}} = (f_1, f_2, \ldots, f_k) \in \mathbb{F}_2^k$ and $\underline{\boldsymbol{c}} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$ denote the message vector and the codeword vector, respectively. The encoding can be described as $\underline{\boldsymbol{c}} = \underline{\boldsymbol{f}} \cdot \mathbf{G}$. Let us assume that a codeword $\underline{\boldsymbol{c}}$ is transmitted by the use of binary phase shift keying (BPSK) modulation

as : $0 \mapsto 1$; $1 \mapsto -1$. The modulated symbol vector is $\underline{\boldsymbol{x}} = (x_1, x_2, \ldots, x_n)$, where $x_j \in \{-1, 1\}$, $\forall j$. Over the additive white Gaussian noise (AWGN) channel, the received symbol vector can be denoted as $\underline{\boldsymbol{r}} = (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$. where

$$r_j = x_j + w_j, \tag{1}$$

and w_j is the AWGN with zero mean and variance $N_0/2$. Let $\Pr(r_j \mid c_j = 0)$ and $\Pr(r_j \mid c_j = 1)$ denote channel observations of c_j, its received LLR is defined as

$$L_j = \ln \frac{\Pr(r_j \mid c_j = 0)}{\Pr(r_j \mid c_j = 1)}. \tag{2}$$

Accordingly, the hard-decision received word $\underline{\boldsymbol{y}} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ can be obtained as

$$y_j = \begin{cases} 0, & \text{if } L_j > 0; \\ 1, & \text{if } L_j \leq 0. \end{cases} \tag{3}$$

Note that a greater $|L_j|$ indicates the received information of c_j is more reliable. Hence, reliability of the received information of all coded bits can be ordered based on $|L_j|$, yielding a refreshed bit index sequence $j_1, j_2, \ldots, j_n$, where

$$|L_{j_1}| \geq |L_{j_2}| \geq \cdots \geq |L_{j_n}|. \tag{4}$$

Subsequently, a sorted received word can be written as

$$\underline{\boldsymbol{y}}' = \Pi\left(\underline{\boldsymbol{y}}\right) = \left(y_{j_1}, y_{j_2}, \ldots, y_{j_n}\right), \tag{5}$$

where Π is the permutation function. Applying the same permutation to the columns of $\mathbf{G}$ yields

$$\mathbf{G}' = \Pi\left(\mathbf{G}\right) = \left[\boldsymbol{g}_{j_1}, \boldsymbol{g}_{j_2}, \ldots, \boldsymbol{g}_{j_n}\right]. \tag{6}$$

The GE will be performed on $\mathbf{G}'$, reducing the first k columns of $\mathbf{G}'$ into weight-one and yielding a systematic generator matrix as

$$\widetilde{\mathbf{G}}' = \left[\boldsymbol{g}'_{j_1}, \boldsymbol{g}'_{j_2}, \ldots, \boldsymbol{g}'_{j_n}\right], \tag{7}$$

where columns $\boldsymbol{g}'_{j_1}, \boldsymbol{g}'_{j_2}, \ldots, \boldsymbol{g}'_{j_k}$ form a $k \times k$ identity submatrix. Note that this process requires the first k columns of $\mathbf{G}'$ being linearly independent. Therefore, the above mentioned permutation needs to be adjusted to ensure this property and $\underline{\boldsymbol{y}}'$ should be updated accordingly. Without further mentioning, we assume that the first k columns of $\mathbf{G}'$ have been ensured with this property. Therefore, the first k positions in $\underline{\boldsymbol{y}}'$ are called the MRIPs and their index set is denoted as $\Upsilon = \{j_1, j_2, \ldots, j_k\}$.

Let $\underline{\boldsymbol{f}}^{(0)}$ denote the initial message corresponding to the first k positions of $\underline{\boldsymbol{y}}'$, i.e., $\underline{\boldsymbol{f}}^{(0)} = (y_{j_1}, y_{j_2}, \ldots, y_{j_k})$. The initial codeword candidate can be obtained by

$$\underline{\boldsymbol{c}}^{(0)} = \Pi^{-1}(\underline{\boldsymbol{f}}^{(0)}\widetilde{\mathbf{G}}'), \tag{8}$$

where Π^{-1} is the inverse of permutation function Π. Let $\underline{\boldsymbol{e}}^{(\omega)} = (e_1^{(\omega)}, e_2^{(\omega)}, \ldots, e_k^{(\omega)}) \in \mathbb{F}_2^k$ denote a TEP that will be added to update $\underline{\boldsymbol{f}}^{(0)}$, where $\omega = 1, 2, \ldots, \sum_{\lambda=1}^{\tau} \binom{k}{\lambda}$, and τ denote the OSD order. Each TEP $\underline{\boldsymbol{e}}^{(\omega)}$ has at most τ non-zero entries. Subsequently, test messages can be generated by

$$\underline{\boldsymbol{f}}^{(\omega)} = \underline{\boldsymbol{f}}^{(0)} + \underline{\boldsymbol{e}}^{(\omega)}. \tag{9}$$

The corresponding codeword candidate can be generated by

$$\hat{\underline{\boldsymbol{c}}}^{(\omega)} = \Pi^{-1}(\underline{\boldsymbol{f}}^{(\omega)}\widetilde{\mathbf{G}}'), \tag{10}$$

where $\hat{\underline{\boldsymbol{c}}}^{(\omega)} = (\hat{c}_1^{(\omega)}, \hat{c}_2^{(\omega)}, \ldots, \hat{c}_n^{(\omega)}) \in \mathbb{F}_2^n$ is the codeword candidate w.r.t. the TEP $\underline{\boldsymbol{e}}^{(\omega)}$. Let us further define the correlation distance between $\underline{\boldsymbol{y}}$ and $\hat{\underline{\boldsymbol{c}}}^{(\omega)}$ as

$$\mathcal{D}(\underline{\boldsymbol{y}}, \hat{\underline{\boldsymbol{c}}}^{(\omega)}) \triangleq \sum_{j: y_j \neq \hat{c}_j^{(\omega)}} |L_j|. \tag{11}$$

If a codeword candidate $\hat{\underline{\boldsymbol{c}}}^{(\omega)}$ yields a smaller correlation distance with $\underline{\boldsymbol{y}}$, it is more likely to be the transmitted codeword. Hence, among all the codeword candidates, the one that yields the smallest correlation distance with $\underline{\boldsymbol{y}}$ will be selected as the decoding output and denoted as $\hat{\underline{\boldsymbol{c}}}_{\text{opt}}$.

III. Reduced complexity Ordered Statistics Decoding

This section introduces the proposed reduced complexity OSD. In order to utilize more information and facilitate the decoding, a validation band is first introduced for the ordered reliability sequence. With this, the validation rule is further proposed to skip the generation of unpromising codeword candidates.

A. Validation Band

With the sorted received word $\underline{\boldsymbol{y}}'$ of (5), let us first define $\Gamma = \{j_1, j_2, \ldots, j_\mu\}$ as the index set of its μ most reliable positions, where $0 \leq \mu \leq n - k$. Note that if $\mu = 0$, $\Gamma = \varnothing$. Our research statistics has shown that these coded bits have an extremely high probability to be error-free, especially when μ is small. Hence, these μ most reliable positions form a validation band, which is denoted as VB. It will be utilized to identify the unpromising codeword candidates. Note that length of the VB can significantly affect the complexity of the proposed OSD and its trade off with the decoding performance. More details on this will be provided in the Section IV.

With the above mentioned VB, the MRIPs that determine the systematic generator matrix should be adjusted accordingly. Different from the conventional OSD [2], the GE will be performed on the permuted generator matrix $\mathbf{G}'$, reducing columns $\boldsymbol{g}_{j_{\mu+1}}, \boldsymbol{g}_{j_{\mu+2}}, \ldots, \boldsymbol{g}_{j_{\mu+k}}$ into weight-one and yielding a systematic generator matrix as

$$\widetilde{\mathbf{G}}'' = \left[\boldsymbol{g}''_{j_1}, \boldsymbol{g}''_{j_2}, \ldots, \boldsymbol{g}''_{j_n}\right], \tag{12}$$

where columns $\boldsymbol{g}''_{j_{\mu+1}}, \boldsymbol{g}''_{j_{\mu+2}}, \ldots, \boldsymbol{g}''_{j_{\mu+k}}$ form a $k \times k$ identity submatrix. Note that we also assume columns $\boldsymbol{g}''_{j_{\mu+1}}, \boldsymbol{g}''_{j_{\mu+2}}, \ldots, \boldsymbol{g}''_{j_{\mu+k}}$ have been ensured with the linearly independent property. Hence, the positions from $\mu + 1$ to $\mu + k$ in $\underline{\boldsymbol{y}}'$ are called the RRIPs and denoted as $\Theta = \{j_{\mu+1}, j_{\mu+2}, \ldots, j_{\mu+k}\}$. Let $\Lambda = \{j_{\mu+k+1}, j_{\mu+k+2}, \ldots, j_n\}$

denote the remaining positions (RPs). For better illustration, the above mentioned index sets are shown in Fig. 1.

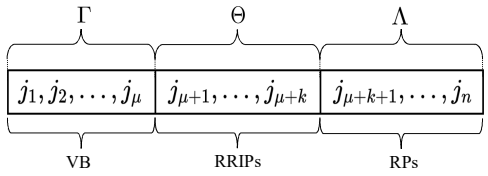

Fig. 1. Index sets of the proposed OSD.

B. Validation Rule

After determining the RRIPs, the initial message $\underline{\boldsymbol{f}}'^{(0)}$ can be obtained accordingly, i.e., $\underline{\boldsymbol{f}}'^{(0)} = (y_{j_{\mu+1}}, y_{j_{\mu+2}}, \ldots, y_{j_{\mu+k}})$. Similarly, the TEP $\underline{\boldsymbol{e}}^{(\omega)} = (e_1^{(\omega)}, e_2^{(\omega)}, \ldots, e_k^{(\omega)}) \in \mathbb{F}_2^k$ will be added to $\underline{\boldsymbol{f}}'^{(0)}$ and generate the test message $\underline{\boldsymbol{f}}'^{(\omega)}$ as

$$\underline{\boldsymbol{f}}'^{(\omega)} = \underline{\boldsymbol{f}}'^{(0)} + \underline{\boldsymbol{e}}^{(\omega)}. \tag{13}$$

The corresponding codeword candidate $\hat{\underline{\boldsymbol{c}}}^{(\omega)} = (\hat{c}_1^{(\omega)}, \hat{c}_2^{(\omega)}, \ldots, \hat{c}_n^{(\omega)}) \in \mathbb{F}_2^n$ can be generated by

$$\hat{\underline{\boldsymbol{c}}}^{(\omega)} = \Pi^{-1}(\underline{\boldsymbol{f}}'^{(\omega)}\widetilde{\mathbf{G}}''), \tag{14}$$

where

$$\hat{c}_j^{(\omega)} = \underline{\boldsymbol{f}}'^{(\omega)} \cdot \boldsymbol{g}_j''. \tag{15}$$

Note that with the statistic property of $\mathbf{G}''$, only the coded bits of the VB and RPs, i.e., $\hat{c}_j^{(\omega)}$ and $j \in \{\Gamma \cup \Lambda\}$, need to be further determined in this re-encoding process. Based on the above analysis, we know that the received bits in the VB, i.e., y_j and $j \in \Gamma$, have an extremely high probability to be error-free. Therefore, coded bits $\hat{c}_j^{(\omega)}$ and $\forall j \in \Gamma$ should have a high priority to be validated as below.

Validation Rule : In the re-encoding process, the coded bits in the VB are prioritized to be estimated by (15). If the coded bits in the VB satisfy

$$\underline{\boldsymbol{f}}'^{(\omega)} \cdot \boldsymbol{g}_j'' = y_j, \forall j \in \Gamma, \tag{16}$$

the re-encoding process will continue and the coded bits in the RPs will be further determined by (15). Otherwise, the test message $\underline{\boldsymbol{f}}'^{(\omega)}$ will be considered as not able to generate a promising codeword candidate. and it will be discarded.

In the proposed OSD, only the test messages that satisfy the validation rule as in (16) are utilized to generate the codeword candidates. It is proposed by assuming that there is no error in the μ most reliable positions of $\underline{\boldsymbol{y}}$. It helps eliminate some unpromising test messages and the generation of the codewords. Summarizing the above description, the proposed OSD is shown below as in *Algorithm 1*.

Algorithm 1 Reduced Complexity OSD Algorithm

Input: $\underline{\boldsymbol{r}}$, μ, τ;
Output: $\hat{\underline{\boldsymbol{c}}}_{\text{opt}}$;

```
Compute the LLRs as in (2), and determine y;
Define VB, RRIPs, and determine f'^(0);
Perform the GE to generate G̃'';
For each TEP e^(ω), do
    Generate test message as in (13);
    If the test message satisfies (16)
        Generate the codeword candidate as in (14);
        Include it in the decoding output list;
End for
Select ĉ_opt from the decoding list based on (11);
```

IV. Performance Analysis

This section characterizes the error distribution of the ordered reliability sequence. The decoding error probability upper bound of the proposed OSD will then be derived.

A. Error Distribution of the Ordered Reliability Sequence

For simplicity, given a sequence $\underline{\boldsymbol{z}} = (z_1, z_2, \ldots, z_n)$, we use $[\underline{\boldsymbol{z}}]_a^b$ to denote the subsequence of with entries indexed from a to b, i.e., $[\underline{\boldsymbol{z}}]_a^b = (z_a, z_{a+1}, \ldots, z_b)$, where $1 \le a < b \le n$. Without loss of generality, given an (n, k) binary linear block code, let us assume that the all-zero codeword is transmitted using BPSK modulation. Therefore, the corresponding modulated symbol vector is $\underline{\boldsymbol{x}} = (1, 1, \ldots, 1)$. Over the AWGN channel, the received symbol vector is $\underline{\boldsymbol{r}} = (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, where $r_j = 1 + w_j$, $\forall j$. Due to the statistically independent property of the AWGN w_j, the probability distribution function (pdf) of the received symbol r_j is given by

$$f_{r_j}(u) = \frac{1}{\sqrt{\pi N_0}} e^{-\frac{(u-1)^2}{N_0}}. \tag{17}$$

With BPSK, LLRs defined in (2) can be further simplified into $L_j = 4r_j/N_0, \forall j$. It indicates that with a given signal-to-noise ratio (SNR) $\gamma = 2/N_0$, r_j can be considered as a scaled LLR. In the following analysis, we define $\underline{\boldsymbol{\chi}} = (\chi_1, \chi_2, \ldots, \chi_n)$, where $\chi_j = |r_j|$, as the reliability sequence of the received symbols. The pdf of χ_j is given by

$$f_{\chi_j}(u) = \begin{cases} 0, & \text{if } u < 0; \\ \frac{1}{\sqrt{\pi N_0}}(e^{-\frac{(u+1)^2}{N_0}} + e^{-\frac{(u-1)^2}{N_0}}), & \text{if } u \ge 0. \end{cases} \tag{18}$$

The cumulative distribution function (cdf) of χ_j can be further derived as

$$F_{\chi_j}(u) = \begin{cases} 0, & \text{if } u < 0; \\ 1 - Q(\frac{u+1}{\sqrt{N_0/2}}) - Q(\frac{u-1}{\sqrt{N_0/2}}), & \text{if } u \ge 0, \end{cases} \tag{19}$$

where $Q(u) = \int_u^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{v^2}{2}\right) dv$ is the standard normal tail function.

Let $\underline{\boldsymbol{\chi}}' = (\chi_1', \chi_2', \ldots, \chi_n')$ denote the ordered reliability sequence. It is obtained by sorting entries of $\underline{\boldsymbol{\chi}}$ in a decreasing order, i.e., $\chi_1' \ge \chi_2' \ge \cdots \ge \chi_n'$. Since the unsorted reliability sequence $\underline{\boldsymbol{\chi}}$ is independent and identically distributed (i.i.d.), with the multinomial distribution, the pdf of the jth ordered

reliability χ'_j can be further derived as [12]

$$f_{\chi'_j}(u) = \frac{n!}{(j-1)!(n-j)!} \cdot (1-F_{\chi_j}(u))^{j-1} F_{\chi_j}(u)^{n-j} f_{\chi_j}(u). \tag{20}$$

Similarly, the joint pdf of the ordered reliabilities χ'_a and χ'_b can be obtained by

$$\begin{aligned} f_{\chi'_a,\chi'_b}(u,v) =& \frac{n!}{(a-1)!(b-a-1)!(n-b)!} \\ & \cdot \left(1-F_{\chi_j}(u)\right)^{a-1} \left(F_{\chi_j}(u)-F_{\chi_j}(v)\right)^{b-a-1} \\ & \cdot F_{\chi_j}(v)^{n-b} f_{\chi_j}(u) f_{\chi_j}(v), \end{aligned} \tag{21}$$

where $u \geq v$. Note that in the case of $u < v$, $\chi'_a < \chi'_b$ and $f_{\chi'_a,\chi'_b}(u,v) = 0$.

Lemma 1*([5]):* Let random variable E_a^b denote the number of errors in $[\underline{\boldsymbol{y}}']_a^b$. Conditioning on the ordered reliability $\chi'_{a-1} = u$ and $\chi'_{b+1} = v$, respectively, the probability that the ordered reliabilities subsequence $[\underline{\boldsymbol{\chi}}']_a^b$ results in λ errors in the hard-decision subsequence $[\underline{\boldsymbol{y}}']_a^b$ is

$$p_{E_a^b}(\lambda \mid u,v) = \binom{b-a+1}{\lambda} p(u,v)^{\lambda} (1-p(u,v))^{b-a+1-\lambda}, \tag{22}$$

where

$$p(u,v) = \frac{Q(\frac{-2u-2}{\sqrt{2N_0}}) - Q(\frac{-2v-2}{\sqrt{2N_0}})}{Q(\frac{-2u-2}{\sqrt{2N_0}}) - Q(\frac{-2v-2}{\sqrt{2N_0}}) + Q(\frac{2v-2}{\sqrt{2N_0}}) - Q(\frac{2u-2}{\sqrt{2N_0}})} \tag{23}$$

is the probability that the arbitrary βth ordered reliability χ'_β results in an error in $[\underline{\boldsymbol{y}}']_a^b$, where $u \geq \chi'_\beta \geq v$.

Proof: With $\chi'_{a-1} = u$ and $\chi'_{b+1} = v$, components in the ordered reliability subsequence $[\underline{\boldsymbol{\chi}}']_a^b$ satisfy

$$u \geq \chi'_a \geq \chi'_{a+1} \geq \cdots \geq \chi'_{b-1} \geq \chi'_b \geq v. \tag{24}$$

Since $\underline{\boldsymbol{\chi}}'$ is obtained by ordering $\underline{\boldsymbol{\chi}}$, the $b-a+1$ ordered reliability components in $[\underline{\boldsymbol{\chi}}']_a^b$ correspond to the $b-a+1$ unsorted reliability components in $\underline{\boldsymbol{\chi}}$ uniquely, i.e.,

$$u \geq \chi_{\xi_a} \geq \chi_{\xi_{a+1}} \geq \cdots \geq \chi_{\xi_{b-1}} \geq \chi_{\xi_b} \geq v. \tag{25}$$

For an arbitrary $\chi_{\xi_\beta} = |r_{\xi_\beta}|$, where $a \leq \beta \leq b$ and $u \geq \chi_{\xi_\beta} \geq v$, the probability that the reliability component χ_{ξ_β} results in an error is given by

$$p(u,v) = \frac{\Pr(-u \leq r_{\xi_\beta} \leq -v)}{\Pr(-u \leq r_{\xi_\beta} \leq -v) + \Pr(v \leq r_{\xi_\beta} \leq u)}. \tag{26}$$

Based on (17), the probability $p(u,v)$ can be further derived as

$$p(u,v) = \frac{Q(\frac{-2u-2}{\sqrt{2N_0}}) - Q(\frac{-2v-2}{\sqrt{2N_0}})}{Q(\frac{-2u-2}{\sqrt{2N_0}}) - Q(\frac{-2v-2}{\sqrt{2N_0}}) + Q(\frac{2v-2}{\sqrt{2N_0}}) - Q(\frac{2u-2}{\sqrt{2N_0}})}. \tag{27}$$

Therefore, under the conditions of the ordered reliability components $\chi'_{a-1} = u$ and $\chi'_{b+1} = v$, the probability that the ordered reliabilities subsequence $[\underline{\boldsymbol{\chi}}']_a^b$ results in λ errors is given as in (22). ■

Theorem 2*([5]):* Given the joint pdf $f_{\chi'_a,\chi'_b}(u,v)$ of (21) and the conditional probability function $p_{E_a^b}(\lambda \mid u,v)$ of (22), when $1 < a < b < n$, the probability mass function $p_{E_a^b}(\lambda)$ of E_a^b is

$$p_{E_a^b}(\lambda) = \int_0^\infty \int_0^\infty p_{E_a^b}(\lambda \mid u,v) f_{\chi'_{a-1},\chi'_{b+1}}(u,v) dv du, \tag{28}$$

where $0 \leq \lambda \leq b-a+1$.

Proof: Based on the Bayes' theorem, $p_{E_a^b}(\lambda)$ can be derived by integrating (22) over u and v with $f_{\chi'_a,\chi'_b}(u,v)$. Note that, u and v are values of the ordered reliabilities χ'_{a-1} and χ'_{b+1}. Hence, (28) holds for the case of $1 < a < b < n$. ■

Theorem 3*([5]):* Given the pdf $f_{\chi'_j}(u)$ of (20) and the conditional probability function $p_{E_a^b}(\lambda \mid u,v)$ of (22), when $b < n$, the probability mass function $p_{E_1^b}(\lambda)$ of E_1^b is

$$p_{E_1^b}(\lambda) = \int_0^\infty \binom{b}{\lambda} p(\infty,v)^{\lambda} (1-p(\infty,v))^{b-\lambda} f_{\chi'_{b+1}}(v) dv, \tag{29}$$

where $0 \leq \lambda \leq b$.

Proof: With $\chi'_{b+1} = v$, components in the ordered reliability subsequence $[\underline{\boldsymbol{\chi}}']_1^b$ satisfy

$$\chi'_1 \geq \chi'_2 \geq \cdots \geq \chi'_{b-1} \geq \chi'_b \geq v. \tag{30}$$

Similar to the analysis of (25), they uniquely correspond to the b unsorted reliability components in $\underline{\boldsymbol{\chi}}$. For an arbitrary component in the ordered reliability subsequence $[\underline{\boldsymbol{\chi}}']_1^b$, it has the average error probability $p(\infty,v)$. Hence, $p_{E_1^b}(\lambda)$ can be derived by integrating $p_{E_1^b}(\lambda \mid \infty,v)$ over ∞ and v with $f_{\chi'_{b+1}}(v)$.

■

B. Decoding Performance Analysis

With the above analysis, we can further derive the decoding error probability upper bound of the proposed OSD.

Corollary 4*:* Let $P_{\text{list}}(\mu,\tau)$ denote the probability of the transmitted codeword not seizing included in the decoding output list, after the reprocessing with the VB of length μ and a decoding order τ, $P_{\text{list}}(\mu,\tau)$ can be obtained by

$$P_{\text{list}}(\mu,\tau) = 1 - P_{E_1^\mu}(0) \cdot \sum_{\lambda=0}^{\tau} P_{E_{\mu+1}^{\mu+k}}(\lambda). \tag{31}$$

Proof: Let $P_{\text{RRIPs}}(\tau)$ denote the probability that the number of errors in the hard-decision sequence indexed by the RRIPs is not greater than τ. Let $P_{\text{VB}}(\mu)$ further denote the probability that hard-decision sequence has no error in the VB, i.e., $[\underline{\boldsymbol{y}}']_1^\mu$. Based on the description of Section III, if the number of errors in the hard-decision sequence indexed by the RRIPs is not greater than τ and $[\underline{\boldsymbol{y}}']_1^\mu$ has no error, the transmitted codeword will be included in the decoding list with a VB of length μ and a decoding order τ. Therefore, $P_{\text{list}}(\mu,\tau)$ depends on both $P_{\text{RRIPs}}(\tau)$ and $P_{\text{VB}}(\mu)$, i.e.,

$$P_{\text{list}}(\mu,\tau) = 1 - P_{\text{RRIPs}}(\tau) \cdot P_{\text{VB}}(\mu). \tag{32}$$

Based on the analysis of Section IV.A, the probability $P_{\text{RRIPs}}(\tau)$ can be obtained by *Theorem 2* as

$$P_{\text{RRIPs}}(\tau) = \sum_{\lambda=0}^{\tau} P_{E_{\mu+1}^{\mu+k}}(\lambda)$$
$$= \sum_{\lambda=0}^{\tau} \left(\int_0^{\infty} \int_0^{\infty} p_{E_{\mu+1}^{\mu+k}}(\lambda \mid u, v) f_{\chi'_{\mu}, \chi'_{\mu+k+1}}(u, v) dv du \right). \quad (33)$$

Similarly, the probability $P_{\text{VB}}(\mu)$ can be obtained by *Theorem 3* as

$$P_{\text{VB}}(\mu) = P_{E_1^{\mu}}(0) = \int_0^{\infty} (1 - p(\infty, v))^{\mu} f_{\chi'_{\mu+1}}(v) dv. \quad (34)$$

■

Based on the analysis of [2], let $P_{\text{e,OSD}}(\mu, \tau)$, and $P_{\text{e,ML}}$ denote the error probability of the proposed OSD with a VB of length μ and a decoding order τ, and the ML decoding error probability, respectively. The error probability of the proposed OSD is upper bounded by

$$P_{\text{e,OSD}}(\mu, \tau) \leq P_{\text{e,ML}} + P_{\text{list}}(\mu, \tau). \quad (35)$$

Note that $P_{\text{e,ML}}$ primarily depends on the minimum Hamming distance and the number of minimum-weight codewords. If $P_{\text{list}}(\mu, \tau) \ll P_{\text{e,ML}}$, a near-optimal decoding performance can be obtained [10]. Therefore, $P_{\text{list}}(\mu, \tau)$ is regarded as a key indicator for the decoding performance.

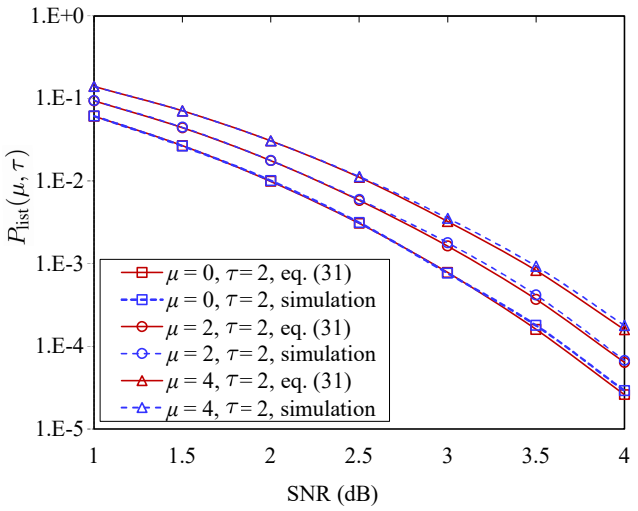

Fig. 2. The probability $P_{\text{list}}(\mu, \tau)$ in decoding the (63, 39) BCH code.

Fig. 2 shows the probability $P_{\text{list}}(\mu, \tau)$ obtained by *Corollary 4* for decoding the (63, 39) BCH code. The decoding simulation results of the code are also provided. It can be seen that *Corollary 4* can accurately characterize the decoding performence of the proposed OSD. Moreover, by adjusting the decoding parameter, i.e., the VB of length μ and the decoding order τ, the decoding performance can be traded with the decoding complexity. More simulation results will be provided in the Section V, shedding more insight on this aspect.

V. Simulation Results

This section provides the numerical results on both the error-correction performance and complexity of the proposed reduced complexity OSD.

A. Decoding Performance

Fig. 3 shows the decoding frame error rate (FER) for the (63, 39) BCH code. The proposed OSD is parameterized by the VB length μ and the decoding order τ. Performance of the conventional OSD [2] and the BMA [9] are provided as comparison benchmarks. The BMA is parameterized by the control band length s and the decoding order τ. The ML decoding performance was obtained from [13]. Our simulation results show that with the same decoding order, the performance of the proposed OSD can approach that of the conventional OSD. By increasing VB length μ, performance of the proposed OSD will only slightly degrade, which is consistent with the results of Fig. 2. The performance loss is incurred by the increased error probability in the VB and more errors might be introduced into RRIPs. Furthermore, Fig. 3 also shows that in decoding the (63, 39) BCH code, the BMA with a control band length of 4 and a decoding order of 1 performs almost the same as the proposed OSD with a VB length of 4 and a decoding order of 2. However, the proposed OSD would be simpler, as discussed below.

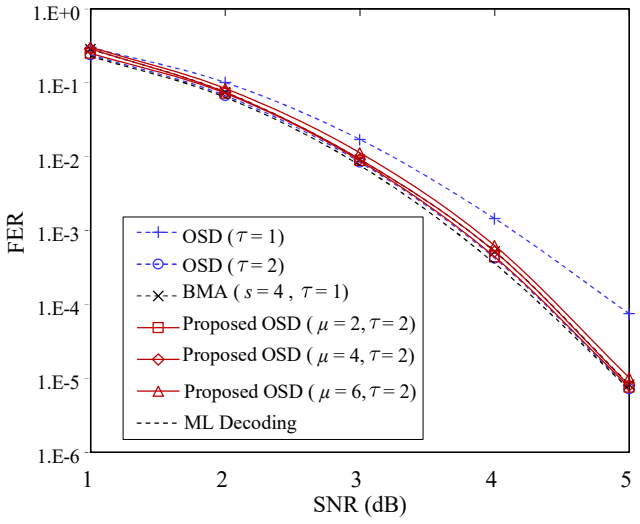

Fig. 3. Decoding performance of the (63, 39) BCH code.

B. Decoding Complexity

Table I compares the complexity of the conventional OSD, the BMA and the proposed OSD in decoding the (63, 39) BCH code. Since the GE is required by all decoding algorithms, for a more intuitive comparison, we only measure the average number of binary operations and floating point operations in the decoding process except the GE. The cardinalities of the decoding output lists are also presented as the supporting evidence. Also referring to Fig. 3, while achieving the near-optimal performance, the proposed OSD exhibits a significant

TABLE I
COMPLEXITY IN DECODING THE (63, 39) BCH CODE

Algorithms	Complexity		Output
	Binary oper.	Floating oper.	list
OSD (τ = 1)	4.19×10^3	5.14×10^2	40
OSD (τ = 2)	1.45×10^5	1.09×10^4	781
BMA (s = 4, τ =1)	1.66×10^4	1.07×10^3	86
Proposed OSD (μ = 2, τ = 2)	3.86×10^4	2.53×10^3	197
Proposed OSD (μ = 4, τ = 2)	1.29×10^4	5.85×10^2	49
Proposed OSD (μ = 6, τ = 2)	6.66×10^3	1.47×10^2	14

complexity advantage. On the one hand, with increasing VB length, the decoding output lists reduces significantly, resulting in a low complexity compared with the conventional OSD. On the order hand, compared with the BMA, when achieving almost the same decoding performance, the proposed OSD yields a lower decoding complexity. Unlike the BMA, the proposed OSD does not require the additional storage, being more implementation friendly. Moreover, by adjusting the decoding parameter, i.e., the VB length μ and the decoding order τ, a trade off between the decoding performance and complexity can be achieved.

VI. CONCLUSION

This paper has proposed a reduced complexity OSD algorithm for linear block codes. By identifying a validation band in several most reliable positions, the generation of the unpromising codeword candidates can be eliminated, resulting in a low decoding complexity. The decoding error probability upper bound of the proposed OSD has also been analyzed. Simulation results have been provided to validate the complexity advantage of the proposed OSD.

ACKNOWLEDGEMENT

This work is sponsored by National Natural Science Foundation of China (NSFC) with project ID 62071498.

REFERENCES

[1] M. C. Coşkun *et al.*, "Efficient error-correcting codes in the short blocklength regime," *Phys. Commun.*, vol. 34, pp. 66–79, 2019.
[2] M. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1379–1396, 1995.
[3] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.
[4] Y. Wu and C. N. Hadjicostis, "Soft-decision decoding using ordered recodings on the most reliable basis," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 829–836, 2007.
[5] C. Yue *et al.*, "A revisit to ordered statistics decoding: distance distribution and decoding rules," *IEEE Trans. Inf. Theory*, vol. 67, no. 7, pp. 4288–4337, 2021.
[6] T, Kaneko *et al.*, "An efficient maximum-likelihood decoding algorithm for linear block codes with algebraic decoder," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 320–327, 1994.
[7] W. Jin and M. Fossorier, "Probabilistic sufficient conditions on optimality for reliability based decoding of linear block codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, July. 2006, Seattle, WA, USA.
[8] C. Yue *et al.*, "Segmentation-discarding ordered-statistic decoding for linear block codes," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, Waikoloa, HI, USA.
[9] A. Valembois and M. Fossorier, "Box and Match techniques applied to soft-decision decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 796–810, 2004.
[10] M. Fossorier, "Reliability-based soft-decision decoding with iterative information set reduction," *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3101–3106, 2002.
[11] W. Jin and M. P. C. Fossorier, "Reliability-based soft-decision decoding with multiple biases," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 105–120, 2007.
[12] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.
[13] Helmling *et al.*, "Database of channel codes and ML simulation results," www.uni-kl.de/channel-codes, 2019.