On the reliability-order-based decoding algorithms for binary linear block codes

Tang, Yuansheng; Ling, San; Fu, Fang-Wei

2006

Tang, Y., Ling, S., & Fu, F. W. (2006). On the reliability-order-based decoding algorithms for binary linear block codes. *IEEE Transactions on Information Theory*, 52(1), 328-336.

<https://hdl.handle.net/10356/96305>

<https://doi.org/10.1109/TIT.2005.860451>

© 2006 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TIT.2005.860451>].

Downloaded on 26 Apr 2023 13:52:19 SGT

On the Reliability-Order-Based Decoding Algorithms for Binary Linear Block Codes

Yuansheng Tang, *Member, IEEE*, San Ling, and Fang-Wei Fu

Abstract—In this correspondence, we consider the decoding of binary block codes over the additive white Gaussian noise (AWGN) channel with binary phase-shift keying (BPSK) signaling. By a reliability-order-based decoding algorithm (ROBDA), we mean a soft-decision decoding algorithm which decodes to the best (most likely) codeword of the form that is the sum of the hard-decision tuple and an error pattern in a set determined only by the order of the reliabilities of the hard decisions. Examples of ROBDA include many well-known decoding algorithms, such as the generalized-minimum-distance (GMD) decoding algorithm, Chase decoding algorithms, and the reliability-based decoding algorithms proposed by Fossorier and Lin. It is known that the squared error-correction-radii of ROBDA can be computed from the minimal squared Euclidean distances (MSEDs) between the all-one sequence and the polyhedra corresponding to the error patterns. For the computation of such MSEDs, we give a new method which is more compact than the one proposed by Fossorier and Lin. These results are further used to show that any bounded-distance ROBDA is asymptotically optimal: The ratio between the probability of decoding error of a bounded-distance ROBDA and that of the maximum-likelihood (ML) decoding approaches 1 when the signal-to-noise ratio (SNR) approaches infinity, provided that the minimum Hamming distance of the code is greater than 2.

Index Terms—Asymptotic optimality, bounded-distance decoding, error performance, linear block codes, maximum-likelihood (ML) decoding, reliability-order-based decoding.

I. INTRODUCTION

For the decoding of binary linear block codes over the additive white Gaussian noise (AWGN) channel with binary phase-shift keying (BPSK) signaling, many soft-decision decoding algorithms, which provide various tradeoffs between the error performance and the decoding complexity, have been proposed in the literature. For some of them, the decoded codeword is selected as the best (most likely) codeword in a list of candidate codewords. In this correspondence, by a *reliability-order-based decoding algorithm* (ROBDA) we mean a soft-decision decoding algorithm whose candidate codewords are the codewords of the form that is the sum of the hard-decision tuple and an error pattern in a set determined only by the order of the reliabilities of the hard decisions. Examples of ROBDA include many well-known

decoding algorithms, such as the generalized-minimum-distance (GMD) decoding algorithm [1], Chase decoding algorithms [2], and the reliability-based decoding algorithms [3], [4]. A detailed list of references concerning ROBDA can be found in [5].

In general, it is very difficult to exactly analyze the error performance of a soft-decision decoding algorithm for all *signal-to-noise ratios* (SNRs). In the literature, the method of simulation is usually used to analyze the error performance for moderate SNRs, whereas the *error exponent*, from which an exponentially tight estimation of the probability of decoding error can be obtained, is a commonly employed indicator of the error performance for high SNRs. For some soft-decision decoding algorithms, the error exponents can be computed simply from the *squared error-correction radius* (SECR) [6]. A soft-decision decoding algorithm is called a *bounded-distance* decoding if its error-correction radius is maximized, i.e., it achieves the guaranteed error-correction radius of the code. For any ROBDA, it is shown by Fossorier and Lin [5] that the SECR can be computed from the minimal squared Euclidean distances (MSEDs) between the all-one sequence and some polyhedra corresponding to the error patterns. An iterative method with linear complexity is further proposed in [5] to compute the MSED for a given error pattern. In this correspondence, we propose a new method to compute such MSEDs. Our method is also of linear complexity and more compact than the one given in [5].

To give a tighter estimation of the probability of decoding error for bounded-distance decoding, a quantity named *effective error coefficient* is also introduced in the literature. For high SNRs, the ratio between the probability of decoding error of a bounded-distance decoding algorithm and that of the *maximum-likelihood* (ML) decoding is approximately bounded by the ratio between the effective error coefficients (cf. [7]–[9]). However, it is pointed out in [9], [10] that, as an indicator for the error performance, the effective error coefficient is still not as good as expected. If the minimum Hamming distance of the code is greater than 2, it is proved in [11] that the GMD and Chase decoding algorithms are asymptotically optimal, that is, the ratio between the probability of decoding error of the GMD or any one of the Chase decoding algorithms and that of the ML decoding approaches 1 when the SNR approaches infinity, even though the ratio between their effective error coefficients is much larger than 1. The main result of this correspondence is to generalize this result to the case of bounded-distance ROBDA. We show that any bounded-distance ROBDA is asymptotically optimal provided that the minimum Hamming distance of the code is greater than 2.

This correspondence is organized as follows. In Section II, we give some definitions and notations needed in this correspondence. In Section III, we discuss the computation of the SECRs of ROBDA. In Section IV, we show that any bounded-distance ROBDA is asymptotically optimal in the sense shown in [11]. In Section V, we end with some concluding remarks.

II. PRELIMINARIES

Suppose that a binary $(N, K, d_{\min})$ linear block code C is used for error control over the AWGN channel with BPSK signaling. If the transmitted codeword is $\mathbf{c} = (c_1, c_2, \dots, c_N) \in C$, then the received sequence $\mathbf{r} \in \mathbb{R}^N$ can be written as $\mathbf{s}(\mathbf{c}) + \mathbf{w}$, where

$$\mathbf{s}(\mathbf{c}) \triangleq ((-1)^{c_1}, (-1)^{c_2}, \dots, (-1)^{c_N})$$

is the bipolar sequence corresponding to $\mathbf{c}$ and the components of $\mathbf{w}$ are independent Gaussian random variables with common density function

$$g(w) \triangleq \frac{1}{(\pi N_0)^{1/2}} e^{-w^2/N_0}.$$

Y. Tang is with the College of Mathematical Science, Yangzhou University, Jiangsu 225002, China, and with State Key Laboratory of Mobile Communications, Southeast University, Jiangsu 210096, China (e-mail: ystang@yzu.edu.cn).

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore. He is now with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore (e-mail: lingsan@ntu.edu.sg).

F.-W. Fu is with the Temasek Laboratories, National University of Singapore, Singapore 117508, Republic of Singapore, on leave from the Department of Mathematics, Nankai University, Tianjin 300071, China; E-mail: tsl-fufw@nus.edu.sg.

Communicated by M. P. Fossorier, Associate Editor for Coding Techniques. Digital Object Identifier 10.1109/TIT.2005.860451

Given the transmitted codeword $\mathbf{c}$, the conditional density function of $\mathbf{r}$ is

$$p(\mathbf{r} | \mathbf{c}) = \frac{1}{(\pi N_0)^{N/2}} e^{-d_E(\mathbf{r}, \mathbf{s}(\mathbf{c}))/N_0} \quad (1)$$

where $d_E(\cdot, \cdot)$ is the *squared Euclidean distance* defined, for sequences $\mathbf{x} = (x_1, x_2, \dots, x_N)$ and $\mathbf{y} = (y_1, y_2, \dots, y_N)$ in $\mathbb{R}^N$, by

$$d_E(\mathbf{x}, \mathbf{y}) \triangleq (x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_N - y_N)^2.$$

The well-known maximum *a posteriori* probability (MAP) decoder outputs the codeword $\mathbf{c}$ which maximizes the *a posteriori* probability $\Pr(\mathbf{c} | \mathbf{r}) = p(\mathbf{r} | \mathbf{c}) \Pr(\mathbf{c}) / p(\mathbf{r})$ for each given $\mathbf{r} \in \mathbb{R}^N$, where $p(\mathbf{r})$ is the density function of the received sequence $\mathbf{r}$ and $\Pr(\mathbf{c})$ is the *a priori* probability that the codeword $\mathbf{c}$ is transmitted. If the codewords are equally likely, i.e., $\Pr(\mathbf{c})$ is the same for all codewords $\mathbf{c}$, maximizing $\Pr(\mathbf{c} | \mathbf{r})$ is equivalent to maximizing $p(\mathbf{r} | \mathbf{c})$. A decoder that outputs the codeword which maximizes $p(\mathbf{r} | \mathbf{c})$ is called a *maximum-likelihood* (ML) decoder.

In general, a soft-decision decoding algorithm A divides $\mathbb{R}^N$ into $2^K + 1$ disjoint regions: $D_A(\mathbf{c})$, for each $\mathbf{c} \in C$ and $\mathcal{F}_A$. If the received sequence $\mathbf{r}$ belongs to $D_A(\mathbf{c})$ for any codeword $\mathbf{c}$ in C , the soft-decision decoding algorithm A declares that $\mathbf{c}$ is the transmitted codeword. If the received sequence $\mathbf{r}$ belongs to $\mathcal{F}_A$, the soft-decision decoding algorithm A makes no decision on the transmitted codeword, i.e., a decoding failure occurs in this case. $D_A(\mathbf{c})$ is called the *decision region* associated with $\mathbf{c}$. For any ML decoder, the inner part of $D_{ML}(\mathbf{c})$ is the *Voronoi region* $V(\mathbf{c})$

$$\{\mathbf{x} \in \mathbb{R}^N : d_E(\mathbf{x}, \mathbf{s}(\mathbf{c})) < d_E(\mathbf{x}, \mathbf{s}(\mathbf{c}'))\}, \text{ for all } \mathbf{c}' \in C \setminus \{\mathbf{c}\}.$$

The error performance analysis of the soft-decision decoding algorithm A is then to estimate the probability that A fails to make the correct decision

$$\Pr(e_A) \triangleq \sum_{\mathbf{c} \in C} \Pr(\mathbf{r} \in D_A^c(\mathbf{c}) | \mathbf{c}) \Pr(\mathbf{c}) \quad (2)$$

where $D_A^c(\mathbf{c}) \triangleq \mathbb{R}^N \setminus D_A(\mathbf{c})$. The MAP decoder is optimal since it minimizes the probability $\Pr(e_A)$. In the meanwhile, if the codewords are not equally likely, an ML decoder is not necessarily optimal. However, in many cases, the *a priori* probabilities are not available at the receiver and then an ML decoder is the best feasible one since the optimal decoding is impossible for such cases.

Let V^N denote the set of binary N -tuples. For a received sequence $\mathbf{r} = (r_1, r_2, \dots, r_N) \in \mathbb{R}^N$, let $\mathbf{z}_\mathbf{r} = (z_1, z_2, \dots, z_N) \in V^N$ denote the hard-decision sequence defined by $z_i = 0$ for $r_i > 0$ and $z_i = 1$ for $r_i \leq 0$. A tuple $\mathbf{v} \in V^N$ is said to be *better under the ML decoding criterion* (or simply *better*) than another tuple $\mathbf{v}' \in V^N$ if $d_E(\mathbf{r}, \mathbf{s}(\mathbf{v})) < d_E(\mathbf{r}, \mathbf{s}(\mathbf{v}'))$. Thus, $\mathbf{z}_\mathbf{r}$ is the best tuple in V^N . We note that maximizing $p(\mathbf{r} | \mathbf{c})$ is equivalent to minimizing $d_E(\mathbf{r}, \mathbf{s}(\mathbf{c}))$. Hence, an ML decoder outputs the best codeword for each received sequence.

Let Λ_N be the set of permutations of $\{1, 2, \dots, N\}$. A permutation $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_N) \in \Lambda_N$ permutes any N -tuple $\mathbf{v} = (v_1, v_2, \dots, v_N)$ into the N -tuple $\lambda(\mathbf{v}) = (v_{\lambda_1}, v_{\lambda_2}, \dots, v_{\lambda_N})$. For any $\lambda \in \Lambda_N$ and any set B of N -tuples, denote

$$\lambda(B) = \{\lambda(\mathbf{b}) : \mathbf{b} \in B\}.$$

For any $\mathbf{x} = (x_1, x_2, \dots, x_N) \in \mathbb{R}^N$, let $\lambda_\mathbf{x} = (\lambda_1, \lambda_2, \dots, \lambda_N) \in \Lambda_N$ be the permutation such that the absolute values of the entries of $\lambda(\mathbf{x})$ are in descending order

$$|x_{\lambda_1}| \geq |x_{\lambda_2}| \geq \dots \geq |x_{\lambda_N}| \quad (3)$$

$$\lambda_i < \lambda_{i+1}, \text{ if } |x_{\lambda_i}| = |x_{\lambda_{i+1}}|. \quad (4)$$

For any $\lambda \in \Lambda_N$, let E_λ be a subset of V^N . For $\mathcal{E} \triangleq \{E_\lambda : \lambda \in \Lambda_N\}$, let $\mathcal{A}(\mathcal{E})$ denote the *reliability-order-based decoding algorithm* (ROBDA) which decodes the received sequence $\mathbf{r} \in \mathbb{R}^N$ to the best codeword in the *search region* $S_\mathcal{E}(\mathbf{r}) \triangleq \{\mathbf{z}_\mathbf{r} + \mathbf{e} : \mathbf{e} \in E_{\lambda_\mathbf{r}}\}$ if it contains some codewords and declares decoding failure otherwise. In general, the subsets E_λ are big enough such that $S_\mathcal{E}(\mathbf{r})$ contains at least one codeword for almost all received sequences $\mathbf{r}$. The tuples in E_λ are called *error patterns*. The codewords in the search region $S_\mathcal{E}(\mathbf{r})$ are also called *candidate codewords* generated by $\mathcal{A}(\mathcal{E})$. In practical algorithms, the candidate codewords are usually generated one by one.

An ML decoder can be seen as an ROBDA with $E_\lambda = V^N$ for all $\lambda \in \Lambda_N$. We note that, for many known ROBDAs, such as the GMD decoding algorithm [1] and the Chase decoding algorithms [2], the set $\lambda(E_\lambda)$ is independent of λ . Therefore, after permuting the bits with $\lambda_\mathbf{r}$, such ROBDAs correct fixed error patterns. Clearly, it is more convenient to describe such ROBDAs after permuting the bits with $\lambda_\mathbf{r}$. However, for the specific ROBDAs proposed in [3], [4], the set $\lambda_\mathbf{r}(E_{\lambda_\mathbf{r}})$ is dependent on the *most reliable basis* which may vary for different permutations $\lambda_\mathbf{r}$. Hence, we do not assume that the bits are pre-ordered according to (3) and (4).

Suppose that $A = \mathcal{A}(\mathcal{E})$ is an arbitrary ROBDA. For each codeword $\mathbf{c}$, let $G_A(\mathbf{c})$, called the *generation region* associated with $\mathbf{c}$, denote the set of sequences $\mathbf{x} \in \mathbb{R}^N$ for which $\mathbf{c}$ is contained in $S_\mathcal{E}(\mathbf{x})$

$$G_A(\mathbf{c}) \triangleq \{\mathbf{x} \in \mathbb{R}^N : \mathbf{c} \in S_\mathcal{E}(\mathbf{x})\}.$$

Clearly, a codeword $\mathbf{c}$ is generated as a candidate codeword if and only if the received sequence $\mathbf{r}$ falls in $G_A(\mathbf{c})$. Let $\Pr(e_A^G)$ be the probability that the transmitted codeword is not generated as a candidate codeword

$$\Pr(e_A^G) \triangleq \sum_{\mathbf{c} \in C} \Pr(\mathbf{r} \in G_A^c(\mathbf{c}) | \mathbf{c}) \Pr(\mathbf{c}). \quad (5)$$

The probability $\Pr(e_A)$ defined by (2) can be bounded by (cf. [5], [11])

$$\max \left\{ \Pr(e_A^G), \Pr(e_{ML}) \right\} \leq \Pr(e_A) \leq \Pr(e_A^G) + \Pr(e_{ML}). \quad (6)$$

For two sequences $\mathbf{x} = (x_1, x_2, \dots, x_N)$ and $\mathbf{x}' = (x'_1, x'_2, \dots, x'_N)$ in $\mathbb{R}^N$, write

$$\mathbf{x} \circ \mathbf{x}' \triangleq (x_1 x'_1, x_2 x'_2, \dots, x_N x'_N).$$

For $\mathbf{x} \in \mathbb{R}^N$ and $\mathcal{X} \subset \mathbb{R}^N$, write $\mathbf{x} \circ \mathcal{X} \triangleq \{\mathbf{x} \circ \mathbf{x}' : \mathbf{x}' \in \mathcal{X}\}$. Let $\mathcal{H}_N$ denote the set of sequences $(x_1, x_2, \dots, x_N) \in \mathbb{R}^N$ with

$$x_1 \geq x_2 \geq \dots \geq x_N \geq 0. \quad (7)$$

From the definition of ROBDAs, it is not difficult to show that

$$\Pr(e_A^G) = \sum_{\lambda \in \Lambda_N, \mathbf{e} \in V^N \setminus E_\lambda} \Pr(\mathbf{r} \in \mathbf{s}(\lambda(\mathbf{e})) \circ \mathcal{H}_N | \mathbf{0}). \quad (8)$$

III. SQUARED ERROR-CORRECTION RADIUS OF ROBDA S

The *squared error-correction radius* (SECR) of a decoding algorithm A for a binary linear block code is defined as the largest number, denoted as $\rho(A)$, such that A decodes correctly whenever the received sequence is within squared Euclidean distance $\rho(A)$ of the bipolar sequence corresponding to the transmitted codeword.

For an ROBDA $A = \mathcal{A}(\mathcal{E})$, it is known that the SECR is given by (cf. [5])

$$\rho(A) = \min \{d_{\min}, \min_{\lambda \in \Lambda_N, \mathbf{e} \in V^N \setminus E_\lambda} \sigma(\lambda(\mathbf{e}))\} \quad (9)$$

where, for $\mathbf{v} \in V^N$, $\sigma(\mathbf{v})$ denotes the *minimal squared Euclidean distance* (MSED) between the sequence $\mathbf{s}(\mathbf{v})$ and the sequences in $\mathbb{R}^N$ which satisfy (7), i.e.,

$$\sigma(\mathbf{v}) \triangleq d_E(\mathbf{s}(\mathbf{v}), \mathcal{H}_N). \quad (10)$$

For the computation of the MSEDs $\sigma(\mathbf{v})$, an iterative method has been proposed in [5]. Below, we present a new method with some ideas from [6]. Our method is more compact than the one given in [5].

A tuple $\mathbf{v} = (v_1, v_2, \dots, v_m) \in V^m$ is called *singular* if

$$\sum_{j=1}^i (t(\mathbf{v}) - (-1)^{v_j}) \geq 0, \quad \text{for all } 1 \leq i \leq m \quad (11)$$

where $t(\mathbf{v})$ is defined by

$$t(\mathbf{v}) \triangleq \max \left\{ 0, \frac{1}{m} \sum_{j=1}^m (-1)^{v_j} \right\}. \quad (12)$$

Clearly, for any singular tuple, its leftmost entry is equal to 0 if and only if the tuple itself is the all-zero tuple $\mathbf{0}$.

Lemma 1: If $\mathbf{v}$ is a singular tuple in V^m , then $\mathbf{x} = t(\mathbf{v})\mathbf{1}_m$ is the unique sequence in $\mathcal{H}_m$ such that

$$d_E(\mathbf{s}(\mathbf{v}), \mathbf{x}) = \sigma(\mathbf{v}) \quad (13)$$

where $\mathbf{1}_m$ is the all-one sequence of length m .

Proof: The proof is given in Appendix I. $\square$

From Lemma 1, one can deduce the following corollary easily.

Corollary 1: If $\mathbf{v} \in V^m$ is a singular tuple with l nonzero entries, then

$$\sigma(\mathbf{v}) = \begin{cases} 4l(m-l)/m, & \text{if } 2l < m \\ m, & \text{otherwise.} \end{cases}$$

For $0 \leq j < j' \leq m$ and a tuple $\mathbf{u} = (u_1, u_2, \dots, u_m)$, let $\gamma_{j,j'}(\mathbf{u})$ denote the subtuple $(u_{j+1}, u_{j+2}, \dots, u_{j'})$ of $\mathbf{u}$. Then we have the following theorem.

Theorem 1: For $\mathbf{e} = (e_1, e_2, \dots, e_N) \in V^N$, let $\mathbf{b}(\mathbf{e}) = (b_0, b_1, \dots, b_{p+1})$ be the sequence of integers such that $b_0 = 0 < b_1 < \dots < b_{p+1} = N$ and, for $0 \leq k \leq p$, b_{k+1} is the largest integer satisfying

$$t(\gamma_{b_k, b_{k+1}}(\mathbf{e})) = \max_{b_k < i \leq N} t(\gamma_{b_k, i}(\mathbf{e})). \quad (14)$$

Then we have the following.

- i) The tuples $\gamma_{b_0, b_1}(\mathbf{e}), \gamma_{b_1, b_2}(\mathbf{e}), \dots, \gamma_{b_p, b_{p+1}}(\mathbf{e})$ are singular and

$$1 \geq t(\gamma_{b_0, b_1}(\mathbf{e})) > t(\gamma_{b_1, b_2}(\mathbf{e})) > \dots > t(\gamma_{b_p, b_{p+1}}(\mathbf{e})) \geq 0. \quad (15)$$

- ii) If $e_1 = 0$, then e_{b_1+1} is the first nonzero entry of $\mathbf{e}$. For each k with $1 \leq k \leq p$, $e_{b_k} = 0$ and $e_{b_k+1} = 1$.
- iii) The sequence $\mathbf{y} \in \mathbb{R}^N$ with

$$\gamma_{b_k, b_{k+1}}(\mathbf{y}) = t(\gamma_{b_k, b_{k+1}}(\mathbf{e}))\mathbf{1}_{b_{k+1}-b_k}$$

for all $0 \leq k \leq p$ is the unique sequence in $\mathcal{H}_N$ such that $d_E(\mathbf{s}(\mathbf{e}), \mathbf{y}) = \sigma(\mathbf{e})$. In particular

$$\sigma(\mathbf{e}) = \sum_{k=0}^p \sigma(\gamma_{b_k, b_{k+1}}(\mathbf{e})). \quad (16)$$

Proof: The proof is given in Appendix II. $\square$

According to Theorem 1, the following Algorithm 1 computes the MSED $\sigma(\mathbf{e})$ for any $\mathbf{e} \in V^N$.

Algorithm 1

Input A tuple $\mathbf{e} \in V^N$ whose nonzero entries are at the positions $n_1 < n_2 < \dots < n_l$.

Output The MSED $\sigma(\mathbf{e})$.

Step 1. If $\mathbf{e}$ has no nonzero entry, output 0 and END. Otherwise, set $I = 1, T = 0$ and $n_{l+1} = N + 1$.

Step 2. Find the largest index $J > I$ such that $\max\{((n_J - n_I) - 2(J - I))/(n_J - n_I), 0\}$ is maximized. If the maximum is positive, add $4(J - I)(n_J - n_I - J + I)/(n_J - n_I)$ to T and goto Step 3. Otherwise, output $T + n_J - n_I$ and END.

Step 3. If $J \leq l$, set $I = J$ and goto Step 2. Otherwise, output T and END. $\square$

We note that the indices n_I and n_J in Algorithm 1 correspond to $b_k + 1$ and $b_{k+1} + 1$, respectively. To efficiently compute the SECR of an ROBDA for long codes, we need further the following lemma (cf. [5, p. 694]).

Lemma 2: Let $\mathbf{e}$ and $\mathbf{e}'$ be two binary N -tuples such that the Hamming weight of $\gamma_{0,i}(\mathbf{e})$ is not smaller than that of $\gamma_{0,i}(\mathbf{e}')$ for all $1 \leq i \leq N$. Then, $\sigma(\mathbf{e}) \geq \sigma(\mathbf{e}')$.

For the two tuples $\mathbf{e}$ and $\mathbf{e}'$ in Lemma 2, we write $\mathbf{e} \succeq \mathbf{e}'$. The following two examples show that, to compute the SECRs for many ROBDA, only very few MSEDs need to be computed even if the set $V^N \setminus E_\lambda$ in (9) is very big.

Example 1: The modified GMD decoding algorithm [13], [7] is the ROBDA with

$$V^N \setminus \lambda(E_\lambda) = \{\mathbf{e} \in V^N : \mathbf{e} \succeq \mathbf{e}^*\}, \quad \text{for all } \lambda \in \Lambda_N$$

where $\mathbf{e}^*$ is the binary N -tuple whose nonzero entries are at the position $N - d_{\min}$ and the positions $N - d_{\min} + 2i + 1$ for $0 < i < t_0 \triangleq \lceil d_{\min}/2 \rceil$. Clearly, $\gamma_{0, N-d_{\min}-1}(\mathbf{e}^*) = \mathbf{0}$ and $N - d_{\min} + 2$ is the largest value of l such that $\gamma_{N-d_{\min}-1, l}(\mathbf{e}^*)$ is a singular tuple and $\gamma_{N-d_{\min}+2, N}(\mathbf{e}^*)$ is also a singular tuple. Then, from Theorem 1

$$\mathbf{b}(\mathbf{e}^*) = (0, N - d_{\min} - 1, N - d_{\min} + 2, N).$$

From Corollary 1

$$\begin{aligned} \sigma(\gamma_{0, N-d_{\min}-1}(\mathbf{e}^*)) &= 0 \\ \sigma(\gamma_{N-d_{\min}-1, N-d_{\min}+2}(\mathbf{e}^*)) &= \frac{4 \cdot 1 \cdot (3-1)}{3} = \frac{8}{3} \\ \sigma(\gamma_{N-d_{\min}+2, N}(\mathbf{e}^*)) &= d_{\min} - 2 \end{aligned}$$

and thus, from (16), $\sigma(\mathbf{e}^*) = d_{\min} + 2/3$. Hence, from (9) and Lemma 2, the SECR of the modified GMD decoding algorithm is equal to $d_{\min}$.

Example 2: Some multiple-Chase-like decoding algorithms are proposed in [14]. Like in the case of the original Chase algorithms, the multiple-Chase-like decoding algorithms employ the bounded-distance- $(t_0 - 1)$ binary decoder, which outputs a codeword within Hamming distance $t_0 - 1$ from the input tuple if any, to generate the candidate codewords. For $0 \leq \tau \leq N - t_0$ and binary N -tuple $\mathbf{u}$, Chase $(\tau, \mathbf{u})$ is a 2^τ -stage decoding algorithm with the following feature: At each stage, the bounded-distance- $(t_0 - 1)$ binary decoder is applied to a binary N -tuple, which is obtained by adding $\mathbf{u}$ to an error pattern whose nonzero components are confined in the τ least reliable positions. For a positive integer h , the (h, τ) -Chase decoding is a multiple-Chase-like decoding algorithm consisting of successive

Chase $(\tau, \mathbf{u}^{(i)})$ with $1 \leq i \leq h$, where $\mathbf{u}^{(i)}$, called the i th search center, is the best binary N -tuple among those which are not yet searched by the $(i-1, \tau)$ -Chase decoding. The first search center is the hard-decision tuple $\mathbf{z}_r$. The second search center is (cf. [15])

$$\mathbf{u}^{(2)} = \mathbf{z}_r + \lambda_r^{-1}((\underbrace{0, \dots, 0}_{N-\tau-t_0}, \underbrace{1, \dots, 1}_{t_0}, \underbrace{1, 0, \dots, 0}_{\tau})).$$

Hence, the $(2, \tau)$ -Chase decoding is the ROBDA with $V^N \setminus \lambda(E_\lambda) = \{\mathbf{e} \in V^N : \mathbf{e} \succeq \mathbf{f}\}$ for all $\lambda \in \Lambda_N$, where

$$\mathbf{f} \triangleq (\underbrace{0, \dots, 0}_{N-\tau-\lceil 3t_0/2 \rceil}, \underbrace{1, \dots, 1}_{\lceil t_0/2 \rceil}, \underbrace{0, \dots, 0}_{\lceil t_0/2 \rceil}, \underbrace{1, \dots, 1}_{\lceil t_0/2 \rceil}, \underbrace{1, 0, \dots, 0}_{\tau}).$$

From (9) and Lemma 2, the SECR of $(2, \tau)$ -Chase decoding is equal to the smaller of $d_{\min}$ and $\sigma(\mathbf{f})$. Since $\gamma_{0, N-\tau-\lceil 3t_0/2 \rceil}(\mathbf{f}) = \mathbf{0}$ and $\gamma_{N-\tau-\lceil 3t_0/2 \rceil, N}(\mathbf{f})$ is a singular tuple, it follows from Theorem 1 and Corollary 1 that

$$\begin{aligned} \sigma(\mathbf{f}) &= \sigma(\gamma_{N-\tau-\lceil 3t_0/2 \rceil, N}(\mathbf{f})) \\ &= \begin{cases} \tau + \lceil t_0/2 \rceil + t_0, & \text{if } \tau \leq \lceil t_0/2 \rceil \\ \frac{4t_0(\tau + \lceil t_0/2 \rceil)}{\tau + \lceil t_0/2 \rceil + t_0}, & \text{otherwise.} \end{cases} \end{aligned}$$

Hence, the SECR of $(2, \tau)$ -Chase decoding is equal to $d_{\min}$ if and only if

$$\begin{aligned} \tau &\geq \lfloor d_{\min}/2 \rfloor - \lceil t_0/2 \rceil \\ &= \begin{cases} \lfloor d_{\min}/4 \rfloor - 1, & \text{if } 4 \mid (d_{\min} - 1) \\ \lfloor d_{\min}/4 \rfloor, & \text{otherwise.} \end{cases} \end{aligned}$$

IV. ASYMPTOTIC OPTIMALITY OF BOUNDED-DISTANCE ROBDA

A decoding algorithm A is called a *bounded-distance* decoding if $\rho(A) = d_{\min}$. The GMD and Chase decoding algorithms are examples of bounded-distance decoding. In [11], GMD and Chase decoding algorithms are shown to be asymptotically optimal, i.e., the ratio between the probability of decoding error of the GMD or any one of the Chase decoding algorithms and that of the ML decoding approaches 1 when the SNR approaches infinity. In this section, we show that an ROBDA decoding algorithm is also asymptotically optimal if it is a bounded-distance decoding.

For tuple $\mathbf{v} = (v_1, v_2, \dots, v_m) \in V^m$, let

$$\begin{aligned} \mathcal{P}(\mathbf{v}) &\triangleq \frac{1}{(\pi N_0)^{m/2}} \int_{\mathcal{H}_m} e^{-d_E(\mathbf{x}, \mathbf{s}(\mathbf{v}))/N_0} d\mathbf{x} \\ &= \int_0^\infty g_{v_1}(x_1) dx_1 \int_0^{x_1} g_{v_2}(x_2) dx_2 \cdots \\ &\quad \int_0^{x_{m-1}} g_{v_m}(x_m) dx_m, \end{aligned} \quad (17)$$

where $g_{v_i}(x_i)$ is defined as

$$g_{v_i}(x_i) \triangleq \frac{1}{\sqrt{\pi N_0}} e^{-(x_i - (-1)^{v_i})^2 / N_0}.$$

For any tuple $\mathbf{z} \in V^N$, from (1) and (17)

$$\Pr(\mathbf{r} \in \mathbf{s}(\mathbf{z}) \circ \mathcal{H}_N \mid \mathbf{0}) = \mathcal{P}(\mathbf{z}). \quad (18)$$

Then, for any ROBDA $\mathcal{A}(\mathcal{E})$, from (8) and (18)

$$\Pr(e_{\mathcal{A}(\mathcal{E})}^G) = \sum_{\lambda \in \Lambda_N, \mathbf{e} \in V^N \setminus E_\lambda} \mathcal{P}(\lambda(\mathbf{e})). \quad (19)$$

From now onwards, all the asymptotic estimates are under the condition $N_0 \rightarrow 0$. For the integral $\mathcal{P}(\mathbf{v})$, an asymptotic estimate is given in the following theorem.

Theorem 2: For any singular tuple $\mathbf{v} \in V^m$

$$\mathcal{P}(\mathbf{v}) = O(1) N_0^{\sigma(\mathbf{v})/4} e^{-\sigma(\mathbf{v})/N_0} \quad (20)$$

where $\sigma(\mathbf{v})$ is defined by (10).

Proof: The proof is given in Appendix III. $\square$

The following corollary is deduced from Theorems 1 and 2.

Corollary 2: For any $\mathbf{e} \in V^N$

$$\mathcal{P}(\mathbf{e}) = O(1) N_0^{\sigma(\mathbf{e})/4} e^{-\sigma(\mathbf{e})/N_0}. \quad (21)$$

Proof: Assume that $\mathbf{b}(\mathbf{e}) = (b_0, b_1, \dots, b_{p+1})$ is the sequence defined in Theorem 1. For $0 \leq i \leq p$, since $\gamma_{b_i, b_{i+1}}(\mathbf{e})$ is a singular tuple, from Theorem 2

$$\mathcal{P}(\gamma_{b_i, b_{i+1}}(\mathbf{e})) = O(1) N_0^{\sigma(\gamma_{b_i, b_{i+1}}(\mathbf{e}))/4} e^{-\sigma(\gamma_{b_i, b_{i+1}}(\mathbf{e}))/N_0}. \quad (22)$$

Then, from (16), (22), and

$$\mathcal{P}(\mathbf{e}) \leq \prod_{i=0}^p \mathcal{P}(\gamma_{b_i, b_{i+1}}(\mathbf{e}))$$

the estimate (21) follows. $\square$

Now, from the well-known estimate (cf. [11])

$$\Pr(e_{\text{ML}}) = \left(\frac{A_{d_{\min}}}{2\sqrt{d_{\min}\pi}} + o(1) \right) N_0^{1/2} e^{-d_{\min}/N_0} \quad (23)$$

where $A_{d_{\min}}$ is the number of codewords of Hamming weight $d_{\min}$, we are ready to prove the following theorem.

Theorem 3: Assume that the minimum Hamming distance $d_{\min}$ of the code C is greater than 2 and $\mathcal{A}(\mathcal{E})$ is a bounded-distance reliability-order-based decoding algorithm. Then, when the SNR approaches infinity, $\mathcal{A}(\mathcal{E})$ is asymptotically optimal, i.e.,

$$\Pr(e_{\mathcal{A}(\mathcal{E})}) = (1 + o(1)) \Pr(e_{\text{ML}}), \quad \text{when } N_0 \rightarrow 0. \quad (24)$$

Proof: For all $\lambda \in \Lambda_N$ and $\mathbf{e} \in V^N \setminus E_\lambda$, since $\mathcal{A}(\mathcal{E})$ is a bounded-distance decoding, i.e., $\rho(\mathcal{A}(\mathcal{E})) = d_{\min}$, from (9), $\sigma(\lambda(\mathbf{e})) \geq d_{\min}$, and thus from (21)

$$\mathcal{P}(\lambda(\mathbf{e})) = O(1) N_0^{d_{\min}/4} e^{-d_{\min}/N_0}. \quad (25)$$

Hence, from (19) and (25)

$$\Pr(e_{\mathcal{A}(\mathcal{E})}^G) = O(1) N_0^{d_{\min}/4} e^{-d_{\min}/N_0}. \quad (26)$$

Since the minimum Hamming distance of C is greater than 2, i.e., $d_{\min} > 2$, it follows from (23) and (26) that

$$\Pr(e_{\mathcal{A}(\mathcal{E})}^G) = o(1) N_0^{1/2} e^{-d_{\min}/N_0} = o(1) \Pr(e_{\text{ML}}). \quad (27)$$

Hence, the asymptotic estimate (24) follows from (6) and (27). $\square$

Remark: We note that not all bounded-distance decoding algorithms are asymptotically optimal. An example is the GMD/TP decoding, which is originally proposed in [12] and defined in [7]. It is shown in [7] that the decision region $D_{\text{GMD/TP}}(\mathbf{c})$ associated to any arbitrary codeword $\mathbf{c}$ is the intersection of the $\binom{N}{d_{\min}}$ open half-spaces

$$\{\mathbf{x} \in \mathbb{R}^N : d_E(\mathbf{x}, \mathbf{s}(\mathbf{c})) < d_E(\mathbf{x}, \mathbf{s}(\mathbf{v} + \mathbf{c}))\}$$

for all tuples $\mathbf{v}$ in V^N of Hamming weight $d_{\min}$. It can be shown easily that the GMD/TP decoding is a bounded-distance decoding and

$$\lim_{N_0 \rightarrow 0} \frac{\Pr(e_{\text{GMD/TP}})}{\Pr(e_{\text{ML}})} = \frac{\binom{N}{d_{\min}}}{A_{d_{\min}}}$$

which is greater than 1 in general.

V. CONCLUSION

In this correspondence, we study the reliability-order-based decoding algorithms (ROBDAs) for binary block codes over AWGN channels. In [5], it is shown that the squared error-correction-radii of ROBDAs can be computed from the minimal squared Euclidean distances (MSEDs) from the all-one tuple to some polyhedra. For the computation of such MSEDs, we give a new method which is more compact than the iterative method given in [5]. Some examples are given to illustrate our new method. These results are further used to show the main result of this correspondence: The ratio between the probability of decoding error for any bounded-distance ROBDA and that for the ML decoding approaches 1 when the SNR approaches infinity, provided that the minimal Hamming distance of the code is greater than 2.

APPENDIX I

PROOF OF LEMMA 1

Proof: We consider to prove, for all $\mathbf{y} \in \mathcal{H}_m$, that

$$d_E(\mathbf{s}(\mathbf{v}), \mathbf{y}) - d_E(\mathbf{s}(\mathbf{v}), t(\mathbf{v})\mathbf{1}_m) \geq \sum_{i=1}^m (y_i - t(\mathbf{v}))^2 \quad (\text{A1})$$

which implies that $\mathbf{x} = t(\mathbf{v})\mathbf{1}_m$ is the unique sequence in $\mathcal{H}_m$ satisfying (13).

Assume $\mathbf{v} = (v_1, v_2, \dots, v_m)$. Let $\mathbf{y} = (y_1, y_2, \dots, y_m)$ be an arbitrary sequence in $\mathcal{H}_m$. Define $y_0 \triangleq y_1 + 1$ and $y_{m+1} \triangleq 0$. Then

$$y_0 > y_1 \geq y_2 \geq \dots \geq y_m \geq y_{m+1}. \quad (\text{A2})$$

Let l be an integer with $0 \leq l \leq m$ such that

$$y_l \geq t(\mathbf{v}) \geq y_{l+1}. \quad (\text{A3})$$

Since $0 \leq t(\mathbf{v}) \leq 1$, such l does exist. From the following identity:

$$\begin{aligned} \sum_{i=1}^m a_i b_i &= \sum_{i=1}^{l-1} (a_i - a_{i+1}) \sum_{j=1}^i b_j + a_l \sum_{j=1}^l b_j \\ &\quad + a_{l+1} \sum_{j=l+1}^m b_j + \sum_{i=l+1}^{m-1} (a_{i+1} - a_i) \sum_{j=i+1}^m b_j \end{aligned}$$

we see that

$$\begin{aligned} d_E(\mathbf{s}(\mathbf{v}), \mathbf{y}) - d_E(\mathbf{s}(\mathbf{v}), t(\mathbf{v})\mathbf{1}_m) &= \sum_{i=1}^m ((y_i - t(\mathbf{v}))^2 + 2(y_i - t(\mathbf{v}))(t(\mathbf{v}) - (-1)^{v_i})) \\ &= \sum_{i=1}^m (y_i - t(\mathbf{v}))^2 + 2 \sum_{i=1}^{l-1} (y_i - y_{i+1}) \sum_{j=1}^i (t(\mathbf{v}) - (-1)^{v_j}) \\ &\quad + 2(y_l - t(\mathbf{v})) \sum_{j=1}^l (t(\mathbf{v}) - (-1)^{v_j}) \\ &\quad + 2(y_{l+1} - t(\mathbf{v})) \sum_{j=l+1}^m (t(\mathbf{v}) - (-1)^{v_j}) \\ &\quad + 2 \sum_{i=l+1}^{m-1} (y_{i+1} - y_i) \sum_{j=i+1}^m (t(\mathbf{v}) - (-1)^{v_j}). \end{aligned} \quad (\text{A4})$$

Now we distinguish between two cases.

Case $t(\mathbf{v}) = 0$. From (A2) and (A3), $y_i = 0$ for $i > l$ and, thus, (A1) follows from (11) and (A2)–(A4).

Case $t(\mathbf{v}) > 0$. From (12), $t(\mathbf{v}) = \frac{1}{m} \sum_{j=1}^m (-1)^{v_j}$ and, thus, from (11)

$$\sum_{j=i+1}^m (t(\mathbf{v}) - (-1)^{v_j}) = - \sum_{j=1}^i (t(\mathbf{v}) - (-1)^{v_j}) \leq 0 \quad (\text{A5})$$

for $0 \leq i \leq m$. Then, (A1) follows from (11) and (A2)–(A5). $\square$

APPENDIX II

PROOF OF THEOREM 1

For simplicity, we abbreviate $\gamma_{b_k, b_{k+1}}(\mathbf{e})$ as $\mathbf{f}_k$ in this appendix.

i) For $0 \leq k \leq p$ and any i with $b_k < i \leq b_{k+1}$, from (12) and (14)

$$\begin{aligned} \sum_{j=b_k+1}^i (t(\mathbf{f}_k) - (-1)^{e_j}) &\geq (i - b_k)t(\mathbf{f}_k) - (i - b_k)t(\gamma_{b_k, i}(\mathbf{e})) \geq 0. \end{aligned}$$

Hence, $\mathbf{f}_k$ is a singular tuple.

For $1 \leq k \leq p$, from $b_k < b_{p+1} = N$ and (14)

$$0 \leq t(\gamma_{b_{k-1}, i}(\mathbf{e})) < t(\mathbf{f}_{k-1}), \quad \text{for any } b_k < i \leq N \quad (\text{B1})$$

and thus, from (12)

$$\sum_{j=b_{k-1}+1}^{b_k} (-1)^{e_j} = (b_k - b_{k-1})t(\mathbf{f}_{k-1}). \quad (\text{B2})$$

If there is an integer k with $1 \leq k \leq p$ such that $t(\mathbf{f}_{k-1}) \leq t(\mathbf{f}_k)$, then $t(\mathbf{f}_k)$ is also positive and thus, from (12)

$$\begin{aligned} \sum_{j=b_k+1}^{b_{k+1}} (-1)^{e_j} &= (b_{k+1} - b_k)t(\mathbf{f}_k) \\ &\geq (b_{k+1} - b_k)t(\mathbf{f}_{k-1}). \end{aligned} \quad (\text{B3})$$

From (B2) and (B3)

$$\begin{aligned} & t(\gamma_{b_{k-1}, b_{k+1}}(\mathbf{e})) \\ &= \max \left\{ 0, \frac{1}{b_{k+1} - b_{k-1}} \sum_{j=b_{k-1}+1}^{b_{k+1}} (-1)^{e_j} \right\} \\ &\geq \frac{(b_k - b_{k-1})t(\mathbf{f}_{k-1}) + (b_{k+1} - b_k)t(\mathbf{f}_{k-1})}{b_{k+1} - b_{k-1}} \\ &= t(\mathbf{f}_{k-1}) \end{aligned}$$

which contradicts (B1). Hence, (15) is true.

- ii) If $e_1 = 0$, it is obvious that e_{b_1+1} is the first nonzero entry of $\mathbf{e}$. Let k be an integer with $1 \leq k \leq p$. If $e_{b_k+1} = 0$, from (12), (B1) and (B2),

$$\begin{aligned} & t(\gamma_{b_{k-1}, b_{k+1}}(\mathbf{e})) \\ &= \max \left\{ 0, \frac{1}{b_k + 1 - b_{k-1}} \sum_{i=b_{k-1}+1}^{b_{k+1}} (-1)^{e_i} \right\} \\ &= \frac{(b_k - b_{k-1})t(\mathbf{f}_{k-1}) + 1}{b_k + 1 - b_{k-1}} \geq t(\mathbf{f}_{k-1}) \end{aligned}$$

which contradicts (14). Hence, $e_{b_k+1} = 1$.

Suppose $e_{b_k} = 1$. If $b_k = b_{k-1} + 1$, it follows from (B2) that $t(\mathbf{f}_{k-1}) = -1$, which contradicts (12). If $b_k - b_{k-1} \geq 2$, from (12) and (B2)

$$\begin{aligned} t(\mathbf{f}_{k-1}) &\leq \frac{(b_k - 1 - b_{k-1})t(\gamma_{b_{k-1}, b_{k-1}}(\mathbf{e})) - 1}{b_k - b_{k-1}} \\ &< t(\gamma_{b_{k-1}, b_{k-1}}(\mathbf{e})), \end{aligned}$$

which contradicts (14). Hence, $e_{b_k} = 0$.

- iii) It follows from (15) that the sequence $\mathbf{y}$ belongs to $\mathcal{H}_N$. Hence,

$$\sigma(\mathbf{e}) \leq d_E(\mathbf{s}(\mathbf{e}), \mathbf{y}) = \sum_{k=0}^p d_E(\mathbf{s}(\mathbf{f}_k), t(\mathbf{f}_k) \mathbf{1}_{b_{k+1}-b_k}). \quad (\text{B4})$$

Let $\mathbf{x}$ be an arbitrary sequence in $\mathcal{H}_N$ such that

$$d_E(\mathbf{s}(\mathbf{e}), \mathbf{x}) = \sigma(\mathbf{e}). \quad (\text{B5})$$

For $0 \leq k \leq p$, since $\mathbf{f}_k$ is singular, from Lemma 1 and $\gamma_{b_k, b_{k+1}}(\mathbf{x}) \in \mathcal{H}_{b_{k+1}-b_k}$

$$\begin{aligned} & d_E(\mathbf{s}(\mathbf{f}_k), t(\mathbf{f}_k) \mathbf{1}_{b_{k+1}-b_k}) \\ &= \sigma(\mathbf{f}_k) \leq d_E(\mathbf{s}(\mathbf{f}_k), \gamma_{b_k, b_{k+1}}(\mathbf{x})). \end{aligned}$$

Hence, from (B4)–(B6),

$$\begin{aligned} \sigma(\mathbf{e}) &\leq \sum_{k=0}^p \sigma(\mathbf{f}_k) \leq \sum_{k=0}^p d_E(\mathbf{s}(\mathbf{f}_k), \gamma_{b_k, b_{k+1}}(\mathbf{x})) \\ &= d_E(\mathbf{s}(\mathbf{e}), \mathbf{x}) = \sigma(\mathbf{e}) \end{aligned}$$

and thus (16) follows. In particular, for all $0 \leq k \leq p$, we have

$$\sigma(\mathbf{f}_k) = d_E(\mathbf{s}(\mathbf{f}_k), \gamma_{b_k, b_{k+1}}(\mathbf{x}))$$

and, therefore, from Lemma 1 and that $\mathbf{f}_k$ is singular

$$\gamma_{b_k, b_{k+1}}(\mathbf{x}) = t(\mathbf{f}_k) \mathbf{1}_{b_{k+1}-b_k} = \gamma_{b_k, b_{k+1}}(\mathbf{y}).$$

Hence, $\mathbf{x} = \mathbf{y}$. This proves the uniqueness of $\mathbf{y}$. $\square$

APPENDIX III PROOF OF THEOREM 2

We first define, for a nonnegative number t

$$\begin{aligned} S(t, N_0) &\triangleq \int_0^\infty g_1(x) \left(\int_0^x g_0(y) dy \right)^t dx \\ &= \frac{1}{(\pi N_0)^{(1+t)/2}} \int_0^\infty \left(\int_0^x e^{-(y-1)^2/N_0} dy \right)^t \\ &\quad \times e^{-(x+1)^2/N_0} dx \\ &= \frac{1}{(\pi N_0)^{(1+t)/2}} \int_1^\infty \left(\int_{2-u}^1 e^{-v^2/N_0} dv \right)^t e^{-u^2/N_0} du. \end{aligned} \quad (\text{C1})$$

To prove Theorem 2, we need some asymptotic estimates for $S(t, N_0)$ when N_0 approaches 0. The following two asymptotic estimates are shown in [11]:

$$S(0, N_0) = \left(\frac{1}{2\sqrt{\pi}} + o(1) \right) N_0^{1/2} e^{-1/N_0} \quad (\text{C2})$$

$$S(1, N_0) = \left(\frac{1}{4\sqrt{2\pi}} + o(1) \right) N_0^{1/2} e^{-2/N_0}. \quad (\text{C3})$$

To give an asymptotic estimate for $S(t, N_0)$ with $t > 1$, we prove the following lemma first.

Lemma 3:

- i) For any given positive number a

$$\int_a^\infty e^{-u^2/N_0} du = \frac{1 + o(1)}{2a} N_0 e^{-a^2/N_0}. \quad (\text{C4})$$

- ii) For real numbers $t > 1$ and ξ with

$$1 + \xi < \frac{2t}{t+1} < 2 - \xi \quad (\text{C5})$$

we have

$$\int_{1+\xi}^{2-\xi} \phi_t(u) du = \left(\frac{\pi^{1/2}(t+1)^{(2t-1)/2}}{2^t} + o(1) \right) N_0^{1/2} \quad (\text{C6})$$

where

$$\phi_t(u) \triangleq (2-u)^{-t} e^{-(t+1)(u-2t/(t+1))^2/N_0}. \quad (\text{C7})$$

Proof:

- i) The asymptotic estimate (C4) follows from (C1), (C2), and

$$\int_a^\infty e^{-u^2/N_0} du = a \int_1^\infty e^{-x^2 a^2/N_0} dx.$$

- ii) For any positive number τ , write $K(\tau) \triangleq \int_\tau^\infty e^{-(t+1)x^2/N_0} dx$. From (C4) and

$$\int_{-\infty}^\infty e^{-y^2} dy = \sqrt{\pi} \quad (\text{C8})$$

we have

$$K(\tau) = \frac{1+o(1)}{2\tau} \cdot \frac{N_0}{t+1} e^{-\tau^2(t+1)/N_0} = o(1)N_0^{1/2} \quad (\text{C9})$$

$$\begin{aligned} K(-\tau) - K(\tau) &= K(-\infty) - 2K(\tau) \\ &= \left(\frac{N_0}{t+1}\right)^{1/2} \cdot \sqrt{\pi} - o(1)N_0^{1/2}. \end{aligned} \quad (\text{C10})$$

On the other hand, it follows from (C5) that

$$\tau_0 \triangleq \min \left\{ \frac{2t}{t+1} - (1+\xi), (2-\xi) - \frac{2t}{t+1} \right\} > 0.$$

Let τ be a given positive number with $0 < \tau \leq \tau_0$. Then,

$$1+\xi \leq 2t/(t+1) - \tau < 2t/(t+1) + \tau \leq 2-\xi$$

and

$$0 \leq \int_{2t/(t+1)-\tau}^{2-\xi} \phi_t(u) du \leq \xi^{-t} K(\tau) \quad (\text{C11})$$

$$\begin{aligned} 0 &\leq \int_{1+\xi}^{2t/(t+1)-\tau} \phi_t(u) du \leq \left(\frac{2}{t+1} + \tau\right)^{-t} K(\tau) \quad (\text{C12}) \\ &\int_{2t/(t+1)-\tau}^{2t/(t+1)+\tau} \phi_t(u) du \geq \left(\frac{2}{t+1} + \tau\right)^{-t} (K(-\tau) - K(\tau)) \quad (\text{C13}) \end{aligned}$$

$$\int_{2t/(t+1)-\tau}^{2t/(t+1)+\tau} \phi_t(u) du \leq \left(\frac{2}{t+1} - \tau\right)^{-t} (K(-\tau) - K(\tau)). \quad (\text{C14})$$

Thus, (C6) follows from the arbitrariness of τ and (C9) to (C14). $\square$

An asymptotic estimate for $S(t, N_0)$ with $t > 1$ is given in the following lemma.

Lemma 4: For any positive number $t > 1$

$$S(t, N_0) = \left(\frac{(t+1)^{(2t-1)/2}}{4^t \pi^{t/2}} + o(1) \right) N_0^{t/2} e^{-4t/(t+1)N_0}. \quad (\text{C15})$$

Proof: Since $t > 1$, there is a small positive number ξ such that (C5) holds and

$$\min\{1+t(1-\xi)^2, (2-\xi)^2\} > \frac{4t}{t+1}. \quad (\text{C16})$$

In the following, we assume that ξ is such a positive number. From (C4), (C8), and (C16)

$$\begin{aligned} &\int_1^{1+\xi} \left(\int_{2-u}^1 e^{-v^2/N_0} dv \right)^t e^{-u^2/N_0} du \\ &\leq \int_1^{1+\xi} \left((u-1)e^{-(1-\xi)^2/N_0} \right)^t e^{-u^2/N_0} du \\ &\leq \xi^t e^{-t(1-\xi)^2/N_0} \int_1^\infty e^{-u^2/N_0} du \\ &= (\xi^t/2 + o(1)) N_0 e^{-(1+t(1-\xi)^2)/N_0} \\ &= o(1) N_0^{(2t+1)/2} e^{-4t/((t+1)N_0)} \end{aligned} \quad (\text{C17})$$

$$\begin{aligned} &\int_{2-\xi}^\infty \left(\int_{2-u}^1 e^{-v^2/N_0} dv \right)^t e^{-u^2/N_0} du \\ &\leq \int_{2-\xi}^\infty \left(\int_{-\infty}^\infty e^{-v^2/N_0} dv \right)^t e^{-u^2/N_0} du \\ &= (\pi N_0)^{t/2} \int_{2-\xi}^\infty e^{-u^2/N_0} du \\ &= \frac{\pi^{t/2} + o(1)}{2(2-\xi)} N_0^{(t+2)/2} e^{-(2-\xi)^2/N_0} \\ &= o(1) N_0^{(2t+1)/2} e^{-4t/((t+1)N_0)}. \end{aligned} \quad (\text{C18})$$

From (C4), for any positive number ϵ , there is a positive number M_ϵ such that, for $0 < N_0 < M_\epsilon$

$$\left| \int_1^\infty e^{-v^2/N_0} dv - \frac{1}{2} N_0 e^{-1/N_0} \right| \leq \frac{\epsilon}{2} N_0 e^{-1/N_0}$$

and consequently, for any positive number a and $0 < N_0 < a^2 M_\epsilon$

$$\begin{aligned} &\left| \int_a^\infty e^{-v^2/N_0} dv - \frac{1}{2a} N_0 e^{-a^2/N_0} \right| \\ &= a \left| \int_1^\infty e^{-u^2 a^2/N_0} du - \frac{1}{2} \cdot \frac{N_0}{a^2} e^{-a^2/N_0} \right| \\ &\leq \frac{\epsilon}{2a} N_0 e^{-a^2/N_0}. \end{aligned} \quad (\text{C19})$$

For $1 < u < 2$ and $N_0 > 0$, write

$$f(u, N_0) \triangleq \frac{1}{2(2-u)} N_0 e^{-(2-u)^2/N_0}. \quad (\text{C20})$$

Then, for $0 < N_0 < \xi^2 M_\epsilon$ and u with $1+\xi \leq u \leq 2-\xi$, from (C19) and $\xi \leq 2-u \leq 1-\xi$

$$\int_{2-u}^1 e^{v^2/N_0} dv \leq \int_{2-u}^\infty e^{v^2/N_0} dv \leq (1+\epsilon) f(u, N_0) \quad (\text{C21})$$

$$\begin{aligned} \int_{2-u}^1 e^{v^2/N_0} dv &= \int_{2-u}^\infty e^{v^2/N_0} dv - \int_1^\infty e^{v^2/N_0} dv \\ &\geq \frac{1-\epsilon}{2(2-u)} N_0 e^{-(2-u)^2/N_0} - \frac{1+\epsilon}{2} N_0 e^{-1/N_0} \\ &= \frac{1-\epsilon - (1+\epsilon)(2-u)e^{((2-u)^2-1)/N_0}}{2(2-u)} N_0 e^{-(2-u)^2/N_0} \\ &\geq \left(1-\epsilon - (1+\epsilon)(1-\xi)e^{((1-\xi)^2-1)/N_0} \right) f(u, N_0). \end{aligned} \quad (\text{C22})$$

Since $(1-\xi)^2 - 1 = -(2-\xi)\xi < 0$, from (C21) and (C22), there is a positive number M_ϵ^* such that, for $0 < N_0 < M_\epsilon^*$ and $1+\xi \leq u \leq 2-\xi$

$$\left| \int_{2-u}^1 e^{-v^2/N_0} dv - f(u, N_0) \right| \leq 2\epsilon f(u, N_0). \quad (\text{C23})$$

Then, from (C6), (C7), (C20), and (C23)

$$\begin{aligned} &\int_{1+\xi}^{2-\xi} \left(\int_{2-u}^1 e^{-v^2/N_0} dv \right)^t e^{-u^2/N_0} du \\ &= (1+o(1)) \int_{1+\xi}^{2-\xi} \left(\frac{1}{2(2-u)} N_0 e^{-(2-u)^2/N_0} \right)^t e^{-u^2/N_0} du \\ &= (1/2^t + o(1)) N_0^t e^{-4t/(t+1)N_0} \\ &\quad \cdot \int_{1+\xi}^{2-\xi} (2-u)^{-t} e^{-(t+1)(u-2t/(t+1))^2/N_0} du \\ &= \left(\frac{\pi^{1/2}(t+1)^{(2t-1)/2}}{4^t} + o(1) \right) N_0^{(2t+1)/2} e^{-4t/(t+1)N_0}. \end{aligned} \quad (\text{C24})$$

Hence, (C15) follows from (C1), (C17), (C18), and (C24). $\square$

Proof of Theorem 2: If $\mathbf{v} = \mathbf{0}$, then $\sigma(\mathbf{v}) = 0$ and (20) follows from the fact that $0 \leq \mathcal{P}(\mathbf{v}) \leq 1$. Now we consider the case that $\mathbf{v}$ has at least one nonzero entry. Assume that the nonzero entries of $\mathbf{v}$ are at the positions $m_1 = 1 < m_2 < \dots < m_l$, where l is the number of the nonzero entries of $\mathbf{v}$. Clearly, for $1 \leq j \leq l$, in the entries of $\mathbf{v}$ at the leftmost $(m_j - 1)$ positions, there are $(j - 1)$ ones and $(m_j - j)$ zeros, respectively. We distinguish between two cases.

Case $2l \geq m$. From (12) and Corollary 1, $t(\mathbf{v}) = 0$ and $\sigma(\mathbf{v}) = m$. For $2 \leq j \leq l$, from (11) and $t(\mathbf{v}) = 0$

$$0 \leq \sum_{i=1}^{m_j-1} (t(\mathbf{v}) - (-1)^{v_i}) = (j-1) - (m_j - j)$$

which implies that $\mathbf{v}$ has at most $(j-1)$ zero entries at the leftmost (m_j-1) positions. Assume that the zero entries of $\mathbf{v}$ are at the positions $n_1 < n_2 < \dots < n_{m-l}$. Then

$$n_j > m_j, \quad \text{for } 1 \leq j \leq m-l. \quad (\text{C25})$$

Since

$$\begin{aligned} \mathcal{P}(\mathbf{v}) &= \int_0^\infty g_1(x_{m_1}) dx_{m_1} \\ &\times \int_0^{x_{m_1}-1} g_1(x_{m_2}) dx_{m_2} \cdots \int_0^{x_{m_l}-1} g_1(x_{m_l}) dx_{m_l} \\ &\times \int_0^{x_{n_1}-1} g_0(x_{n_1}) dx_{n_1} \cdots \int_0^{x_{n_{m-l}}-1} g_0(x_{n_{m-l}}) dx_{n_{m-l}} \end{aligned} \quad (\text{C26})$$

from (C2), (C3), and (C25)

$$\begin{aligned} \mathcal{P}(\mathbf{v}) &\leq \int_0^\infty g_1(x_{m_1}) dx_{m_1} \\ &\times \int_0^{x_{m_1}} g_1(x_{m_2}) dx_{m_2} \cdots \int_0^{x_{m_l}} g_1(x_{m_l}) dx_{m_l} \\ &\times \int_0^{x_{m_1}} g_0(x_{n_1}) dx_{n_1} \cdots \int_0^{x_{m-l}} g_0(x_{n_{m-l}}) dx_{n_{m-l}} \\ &\leq (S(1, N_0))^{m-l} \cdot (S(0, N_0))^{l-(m-l)} \\ &= O(1) N_0^{l/2} e^{-m/N_0}. \end{aligned} \quad (\text{C27})$$

Then, the estimate (20) follows from $2l \geq m = \sigma(\mathbf{v})$ and (C27).

Case $2l < m$. From (12) and Corollary 1, $t(\mathbf{v}) = (m-2l)/m$ and $\sigma(\mathbf{v}) = 4l(m-l)/m$. For any $2 \leq j \leq l$, from (11)

$$\begin{aligned} \sum_{i=1}^{m_j-1} (t(\mathbf{v}) - (-1)^{v_i}) \\ = (m_j-1) \cdot \frac{m-2l}{m} - ((m_j-j) - (j-1)) \geq 0 \end{aligned}$$

which is equivalent to

$$m_j - j \leq \frac{(j-1)(m-l)}{l}. \quad (\text{C28})$$

The inequality (C28) implies that the number of zero entries of $\mathbf{v}$ at the leftmost (m_j-1) positions is not greater than $\lfloor (j-1)(m-l)/l \rfloor$ or, in other words, the $(\lfloor (j-1)(m-l)/l \rfloor + 1)$ th zero entry of $\mathbf{v}$ must be to the right of the j th nonzero entry of $\mathbf{v}$. Hence, from (C15), (C26), and (C28)

$$\begin{aligned} \mathcal{P}(\mathbf{v}) &\leq \int_0^\infty g_1(x_{m_1}) dx_{m_1} \\ &\int_0^{x_{m_1}} g_1(x_{m_2}) dx_{m_2} \cdots \int_0^{x_{m_l}-1} g_1(x_{m_l}) dx_{m_l} \\ &\left(\int_0^{x_{m_1}} g_0(x) dx \right)^{\lfloor \frac{m-l}{l} \rfloor} \\ &\left(\int_0^{x_{m_2}} g_0(x) dx \right)^{\lfloor \frac{2(m-l)}{l} \rfloor - \lfloor \frac{m-l}{l} \rfloor} \\ &\cdots \left(\int_0^{x_{m_l}} g_0(x) dx \right)^{m-l - \lfloor \frac{(l-1)(m-l)}{l} \rfloor} \end{aligned}$$

$$\begin{aligned} &\leq \int_0^\infty g_1(x_{m_1}) dx_{m_1} \\ &\int_0^{x_{m_1}} g_1(x_{m_2}) dx_{m_2} \cdots \int_0^{x_{m_l}-1} g_1(x_{m_l}) dx_{m_l} \\ &\left(\int_0^{x_{m_1}} g_0(x) dx \right)^{\frac{m-l}{l}} \left(\int_0^{x_{m_2}} g_0(x) dx \right)^{\frac{m-l}{l}} \\ &\cdots \left(\int_0^{x_{m_l}} g_0(x) dx \right)^{\frac{m-l}{l}} \\ &\leq \left(S\left(\frac{m-l}{l}, N_0\right) \right)^l \\ &= O(1) N_0^{(m-l)/2} e^{-4l(m-l)/m N_0}. \end{aligned} \quad (\text{C29})$$

Thus, the estimate (20) follows from $2(m-l) > 4l(m-l)/m = \sigma(\mathbf{v})$ and (C29). $\square$

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees and the Associate Editor M. Fossorier for their useful comments and suggestions that helped to improve the correspondence.

REFERENCES

- [1] G. D. Forney Jr., "Generalized minimum distance decoding," *IEEE Trans. Inf. Theory*, vol. IT-12, no. 2, pp. 125–131, Apr. 1966.
- [2] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 1, pp. 170–182, Jan. 1972.
- [3] M. P. C. 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, Sep. 1995.
- [4] —, "Computationally efficient soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 738–750, May 1996.
- [5] —, "A unified method for evaluating the error-correction radius of reliability-based soft-decision algorithms for linear block codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 691–700, Mar. 1998.
- [6] Y. Tang, "On the error exponents of reliability-order-based decoding algorithms for linear block codes," in *Coding Theory, Cryptography & Combinatorics, Progress in Computer Science and Applied Logic*, K. Feng, H. Niederreiter, and C. Xing, Eds. Basel, Switzerland: Birkhäuser-Verlag, 2004, vol. 23, pp. 303–317.
- [7] B. Shen, K. K. Tzeng, and C. Wang, "A bounded-distance decoding algorithm for binary linear block codes achieving the minimum effective error coefficient," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1987–1991, Nov. 1996.
- [8] E. Fishler, O. Amrani, and Y. Be'ery, "Geometrical and performance analysis of GMD and Chase decoding algorithms," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1406–1422, Jul. 1999.
- [9] G. D. Forney and A. Vardy, "Generalized minimum-distance decoding of Euclidean codes and lattices," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1992–2026, Nov. 1996.
- [10] D. Agrawal and A. Vardy, "Generalized minimum distance decoding in Euclidean space: Performance analysis," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 60–83, Jan. 2000.
- [11] Y. Tang, T. Fujiwara, and T. Kasami, "Asymptotic optimality of the GMD and Chase decoding algorithms," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2401–2405, Aug. 2002.
- [12] D. J. Taipale and M. B. Pursley, "An improvement to generalized-minimum-distance decoding," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 167–172, Jan. 1991.
- [13] G. D. Forney Jr., "A bounded-distance decoding algorithm for the Leech lattice, with generalizations," *IEEE Trans. Inf. Theory*, vol. 35, no. 4, pp. 906–909, Jul. 1989.
- [14] T. Kasami, "On integer programming problems related to soft-decision iterative decoding algorithms," in *Proc. 13th Int. Symp. AAECC (Lecture Notes in Computer Science)* Berlin, Germany, 1999, vol. 1719, pp. 43–54.

- [15] Y. Tang, T. Kasami, and T. Fujiwara, "On the computation of the search centers and the evaluation of the testing conditions for the h -chase decoding," in *Proc. 23rd Symp. Information Theory and Its Applications*, Aso, Kumamoto, Japan, Oct. 2000, pp. 77–80.