Reduced GMD Decoding

Jos H. Weber, *Senior Member, IEEE,* and
Khaled A. S. Abdel-Ghaffar, *Member, IEEE*

***Abstract*—A framework is presented for generalized minimum distance (GMD) decoding with a limited number of decoding trials and a restricted set of reliability values. In GMD decoding, symbols received from the channel may be erased before being fed into an algebraic error-erasure decoder for error correction, in subsequent or simultaneous trials with different erasing patterns. The decision whether or not to erase a symbol in a certain trial is taken by an erasure-choosing algorithm which takes into account reliability information from the channel. The final GMD decoder output is a codeword which results from a decoding trial and satisfies a certain distance criterion. For various erasing strategies and reliability sets, the guaranteed error-correction radius and the unsuccessful decoding probability of this technique are studied. Both known and new results, with applications to concatenated coding, follow from the unified approach presented in this correspondence.**

***Index Terms*—Concatenated codes, generalized distance, multitrial decoding, reliability-based decoding.**

I. Introduction

Generalized minimum distance (GMD) decoding, as introduced by Forney [6], [7], permits flexible use of reliability information in algebraic decoding algorithms for error correction. It applies to both binary and nonbinary codes. The main idea is to use a simple algebraic error-erasure decoder in a multitrial fashion, with different erasing patterns based on reliability information from the channel and termination based on a certain distance criterion. In this way, the virtues of probabilistic and algebraic decoding approaches can be combined.

Although GMD decoding is a rather old technique, it is still highly relevant. It is also considered in combination with more modern techniques. For example, in [13], a concatenated coding scheme has been proposed with a turbo inner code and a Reed–Solomon outer code. In case the maximum number of iterations for inner turbo decoding has been reached and outer (hard-decision) decoding is still unsuccessful, the outer decoder computes the reliability values of its input symbols based on the soft output information of the inner turbo decoder and carries out a final GMD-like decoding step.

In this correspondence, we study the effects of reducing the maximum number of decoding trials (as proposed in [12]) and/or reducing the set of allowable reliability values in GMD decoding. The latter may be of importance since, in any digital implementation, the reliability values need to be quantized. Moreover, in some applications, e.g., GMD decoding of concatenated codes over discrete channels, the reliability values are discrete in nature. The proposed limitations on the maximum number of trials and the allowable reliability values may considerably decrease the decoding complexity, but possibly at the expense of performance degradation. A general framework is presented for such *reduced GMD decoders*, with Forney's algorithm (multitrial, broad range of reliability levels) at one side of the spectrum and errors-only decoding (single trial, only one reliability level) at the other side.

Several performance studies and many variations on and extensions or improvements to the GMD decoding principle have been proposed over the years [2], [4], [9], [10], [15], see, e.g., [8] for an overview. Still, we have chosen to refer to Forney's original work in the evaluation of the effects of reducing the number of trials and/or allowable reliability levels. It should be noted, however, that much of the analysis presented here may apply to other GMD-based soft-decision decoding techniques as well.

We assume the following setting. A codeword $\boldsymbol{c} = (c_1, \ldots, c_n)$ from a q-ary code $\mathcal{C}$ of length n and Hamming distance d is transmitted over a channel which may distort the transmitted symbols. Let $\boldsymbol{z} = (z_1, \ldots, z_n)$ be the channel output, where z_i does not necessarily belong to the code alphabet. A detector delivers, for each $i = 1, \ldots, n$, a q-ary symbol r_i, which belongs to the code alphabet, and which represents the detector's estimate of c_i based on z_i, and a reliability value α_i, which belongs to a set $\mathcal{R}$, and which represents the detector's confidence in its estimate. The input to the decoder consists of the received q-ary vector $\boldsymbol{r} = (r_1, \ldots, r_n)$ and the associated reliability vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$.

We assume in the following that $\mathcal{R}$ is a closed subset of the real interval $[0, 1]$ containing $\{1\}$, i.e.,

$$\{1\} \subseteq \mathcal{R} \subseteq [0, 1]. \tag{1}$$

The lower α_i, the less reliable is the symbol r_i, with $\alpha_i = 0$ corresponding to "fully unreliable." Throughout the rest of the correspondence, we will assume without loss of generality, that the ordering of the received symbols is such that $\alpha_i \leq \alpha_{i+1}$ for $i = 1, \ldots n-1$.

Of particular relevance are the families of sets

$$\mathcal{R}_\mu = [\mu, 1] \tag{2}$$

with $\mu \in [0, 1]$, and

$$\mathcal{R}_m = \bigcup_{i=0}^{\lfloor m/2 \rfloor} \{1 - 2i/m\} \tag{3}$$

with $m = 1, 2, 3, \ldots$. These include the simple cases of taking only *hard decisions* ($\mu = 1$ or $m = 1$) and of allowing *erasures* ($m = 2$).

The *generalized distance* between the received word $\boldsymbol{r}$ with reliability vector $\boldsymbol{\alpha}$ and a q-ary vector $\boldsymbol{v} = (v_1, \ldots, v_n)$ is defined as

$$d_{\mathrm{G}}(\boldsymbol{v}, \boldsymbol{r}, \boldsymbol{\alpha}) = \sum_{i:\, v_i = r_i} (1 - \alpha_i)/2 + \sum_{i:\, v_i \neq r_i} (1 + \alpha_i)/2. \tag{4}$$

Note that for $\mathcal{R} = \mathcal{R}_1 = \{1\}$, i.e., $\alpha_i = 1$ for all i, the generalized distance $d_{\mathrm{G}}(\boldsymbol{v}, \boldsymbol{r}, \boldsymbol{\alpha})$ reduces to the Hamming distance $d_{\mathrm{H}}(\boldsymbol{v}, \boldsymbol{r})$ between $\boldsymbol{v}$ and $\boldsymbol{r}$.

Forney [6], [7] has shown that for any $\boldsymbol{r}$ and $\boldsymbol{\alpha}$, there can be at most one codeword $\boldsymbol{c}$ such that

$$d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) < d/2. \tag{5}$$

Furthermore, he has also shown that if a codeword satisfying (5) exists, it will be found by the following simple procedure. In trial j (with initial value $j = 1$), the $2j - 1$ (if d is even) or $2j - 2$ (if d is odd) most unreliable received symbols in $\boldsymbol{r}$ are erased, after which the resulting sequence is fed into an (algebraic) error-erasure decoder with the property that it returns the original codeword whenever the numbers of erasures e and errors t are such that $2t + e < d$. If the error-erasure decoder generates a codeword $\boldsymbol{c}$ satisfying (5), then this codeword is

Manuscript received April 26, 2001; revised November 11, 2002. The work of K. A. S. Abdel-Ghaffar was supported by the National Science Foundation under Grants CCR-0117891 and ECS-0121469. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Sorrento, Italy, June 2000 and the IEEE International Symposium on Information Theory, Washington, DC, June 2001.

J. H. Weber is with the Department ITS, Delft University of Technology, 2600 GA, Delft, The Netherlands (e-mail: J.H.Weber@ITS.TUDelft.NL).

K. A. S. Abdel-Ghaffar is with the Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA (e-mail: ghaffar@ece.ucdavis.edu).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.809504

taken as the final decoding result, else j is increased by 1 and another trial is performed, unless j exceeds $\lceil d/2 \rceil$, in which case the procedure is terminated.

Although Forney's method finds the codeword $\boldsymbol{c}$ (if one exists) satisfying (5) in (at most) $\lceil d/2 \rceil$ trials for *any* reliability set $\mathcal{R}$, the term *generalized minimum distance (GMD) decoding* has been reserved mainly for this procedure in combination with the reliability set $\mathcal{R} = \mathcal{R}_0 = [0, 1]$. For this $\mathcal{R}$, Forney has shown that for binary antipodal signals sent over an additive white Gaussian noise (AWGN) channel, GMD decoding has effectively the same error probability as maximum-likelihood (ML) decoding at high signal-to-noise ratios (SNRs).

Kovalev [12] considered limiting the maximum number of decoding trials to an arbitrary number l less than $\lceil d/2 \rceil$. In this case, the recovery of the transmitted codeword $\boldsymbol{c}$ is guaranteed if and only if the generalized distance $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha})$ is less than some number, which we call the guaranteed error-correction radius achievable by the decoder.

In his work, Kovalev considered fixed erasing strategies, where the number of symbols to be erased in each trial is fixed, and optimized erasing strategies, where this number is optimally chosen, based on the reliability vector $\boldsymbol{\alpha}$, to maximize the guaranteed error-correction radius of the decoder. For the reliability set $\mathcal{R} = [0, 1]$, Kovalev determined or bounded the guaranteed error-correction radius of l-trial decoders employing either fixed erasing strategies or optimized erasing strategies.

In addition to fixed and optimized erasing strategies, we study, in this correspondence, threshold erasing strategies, where the decision of erasing or not erasing a given symbol in a given trial depends on whether or not the reliability of the symbol falls below a certain predetermined threshold. In particular, unlike fixed and optimized erasing strategies, the decision does not depend on the reliabilities of other symbols. Hence, for threshold erasing, the detected symbols need not be ordered in terms of reliability values. By covering threshold erasing strategies, the decoding techniques of concatenated codes developed by Zyablov [16] fit naturally in our framework.

For fixed, threshold, and optimized strategies, we study GMD decoding in case the reliability set $\mathcal{R}$ is a subset of $[0, 1]$. In particular, we focus on the sets $\mathcal{R}_\mu$ and $\mathcal{R}_m$ introduced in (2) and (3), respectively. The (maximum) number of trials l is considered as a parameter that reflects the allowable cost and/or delay of the decoder. Restricting $\mathcal{R}$ and/or l leads to the concept of reduced GMD decoding.

In Section II, we consider the guaranteed error-correction radius in case of such reduced reliability sets. This is the maximum number such that, for any $\boldsymbol{r}$ and $\boldsymbol{\alpha}$, there is at most one codeword $\boldsymbol{c}$ such that $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha})$ is less than this number. From (5), we know that the guaranteed error-correction radius is at least $d/2$. Depending on $\mathcal{R}$ and d, we show that the guaranteed error-correction radius may be larger than $d/2$. In such cases, we have a less stringent criterion to accept the decoder's output. If no codeword satisfying the criterion is found, one can decide to have no decoding result at all (*decoding failure*), or to choose as the final decoding output a codeword generated in one of the trials, which is closest to the received sequence in generalized distance sense. In this correspondence, we assume that the first option is in use, i.e., the original codeword is retrieved if and only if it satisfies the criterion. Although there are even less stringent conditions for some choices of $\boldsymbol{\alpha}$ [5], [14], ours, by definition, cannot be improved upon for all $\boldsymbol{\alpha}$. In particular, employing criteria different from ours may lead to a reduction in decoding failure probability, but has no impact on results that have to consider the worst possible $\boldsymbol{\alpha}$. For this reason, we employ the criterion based on the guaranteed error-correction radius.

Section III describes limited-trial decoding based on arbitrary erasing strategies. In Section IV, the maximum guaranteed error-correction radius achievable by fixed erasing is determined for any reliability set $\mathcal{R}$. This generalizes results in [6], [7], [12]. Section V gives the maximum guaranteed error-correction radius achievable by threshold erasing in the cases $\mathcal{R} = \mathcal{R}_\mu$ or $\mathcal{R} = \mathcal{R}_m$. This generalizes results derived in [16] in the context of concatenated codes. In Section VI, we use the results of Kovalev [12] that give tight bounds on the guaranteed error-correction radius achievable by optimized erasing in case $\mathcal{R} = [0, 1]$, to derive bounds for an arbitrary reliability set $\mathcal{R}$. We also determine the guaranteed error-correction radius achievable by single-trial decoding in the cases $\mathcal{R} = \mathcal{R}_\mu$ or $\mathcal{R} = \mathcal{R}_m$.

Next, in Section VII, we present an asymptotic performance analysis of reduced GMD decoding schemes in case of sending binary antipodal signals over an AWGN channel. Since Forney's GMD decoding scheme with $\mathcal{R} = [0, 1]$ and $l = \lceil d/2 \rceil$ achieves the same performance as ML decoding at high SNRs, we characterize the loss due to restricting the reliability set $\mathcal{R}$ to be a subset of $[0, 1]$ and the loss due to restricting the maximum number of trials l.

GMD decoding is known to be an efficient decoding technique for concatenated codes (see, e.g., [3], [5], [7]). In this context, GMD decoding is performed on the outer code and the reliability values are provided by the inner code decoders. Application of reduced GMD decoding to concatenated codes is considered in Section VIII, where we relate the maximum number of errors that can be corrected by a reduced GMD decoder in a concatenated coding scheme to the guaranteed error-correction radius achievable by the decoder. Finally, the results from the correspondence are discussed in Section IX.

In this correspondence, we use $\wedge$ and $\vee$ for logical "and" and logical "or," respectively. For integers a, b, and m, we write $a \equiv b(m)$ to denote $a \equiv b \pmod m$.

II. Guaranteed Error-Correction Radius

As stated before, Forney [6], [7] has shown that for any received symbol sequence $\boldsymbol{r}$ and reliability sequence $\boldsymbol{\alpha}$, there can be at most one codeword $\boldsymbol{c}$ such that $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) < d/2$. However, $d/2$ may not be the largest number for which this property holds. We denote the largest real number for which the property holds by $r_{\mathrm{G}}(d, \mathcal{R})$. Hence, if the transmitted codeword $\boldsymbol{c}$ and the received sequences $\boldsymbol{r}$ and $\boldsymbol{\alpha}$ satisfy

$$d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) < r_{\mathrm{G}}(d, \mathcal{R}) \tag{6}$$

then $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) < d_{\mathrm{G}}(\boldsymbol{c}', \boldsymbol{r}, \boldsymbol{\alpha})$ for any codeword $\boldsymbol{c}' \neq \boldsymbol{c}$. Therefore, we call $r_{\mathrm{G}}(d, \mathcal{R})$ the *guaranteed error-correction radius*.

As the notation suggests, the guaranteed error-correction radius depends on the code $\mathcal{C}$ only by its Hamming distance d and not by its length or particular structure, which is shown in the following result.

Theorem 1: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$ and a reliability set $\mathcal{R}$, it holds that

$$r_{\mathrm{G}}(d, \mathcal{R}) = d/2 + \min \left| \sum_{i \in \mathcal{J}_1} \kappa_i - \sum_{i \in \mathcal{J}_2} \kappa_i \right| \Big/ 2 \tag{7}$$

where the minimum is over all disjoint sets $\mathcal{J}_1$ and $\mathcal{J}_2$ such that $\mathcal{J}_1 \cup \mathcal{J}_2 = \{1, 2, \ldots, d\}$ and all $\kappa_i \in \mathcal{R}$, $1 \leq i \leq d$.

Proof: Clearly, $r_{\mathrm{G}}(d, \mathcal{R})$ is the minimum of

$$\max\{d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}), d_{\mathrm{G}}(\boldsymbol{c}', \boldsymbol{r}, \boldsymbol{\alpha})\} \tag{8}$$

over all pairs of distinct codewords $\boldsymbol{c}$ and $\boldsymbol{c}'$ from $\mathcal{C}$, all q-ary sequences $\boldsymbol{r}$ of length n, and all $\boldsymbol{\alpha} \in \mathcal{R}^n$. First, suppose that $\boldsymbol{c}$ and $\boldsymbol{c}'$ are given and let $\mathcal{J} = \{i\colon c_i \neq c_i'\}$. Then, in seeking the minimum of (8) over all $\boldsymbol{r}$ and $\boldsymbol{\alpha}$, we may assume that $r_i = c_i = c_i'$ and $\alpha_i = 1$ for all $i \notin \mathcal{J}$, and $r_i = c_i$ or $r_i = c_i'$ for all $i \in \mathcal{J}$. From (4), this minimum equals

$$\left(|\mathcal{J}| + \min \left| \sum_{i \in \mathcal{J}_1} \kappa_i - \sum_{i \in \mathcal{J}_2} \kappa_i \right| \right) \Big/ 2 \tag{9}$$

where the minimum is over all disjoint sets $\mathcal{J}_1$ and $\mathcal{J}_2$ such that $\mathcal{J}_1 \cup \mathcal{J}_2 = \mathcal{J}$ and over all $\kappa_i \in \mathcal{R}$, $i \in \mathcal{J}$. The minimum of (9) over all distinct codewords $\boldsymbol{c}$ and $\boldsymbol{c}'$ is attained if $|\mathcal{J}|$ is minimum, i.e., $|\mathcal{J}| = d$. □

This implicit expression leads to the following explicit bounds.

Corollary 1: For $d \geq 1$ and $\{1\} \subseteq \mathcal{R} \subseteq [0, 1]$, it holds that

$$d/2 \leq r_{\mathrm{G}}(d, \mathcal{R}) \leq (d + \min \mathcal{R})/2 \tag{10}$$

where equality holds in the first inequality if d is even.

Proof: From Theorem 1, $r_{\mathrm{G}}(d, \mathcal{R}) \geq d/2$. If d is even, then the choice $|\mathcal{J}_1| = |\mathcal{J}_2| = d/2$ and $\kappa_i = 1$ for all $i = 1, \ldots, d$ proves that $r_{\mathrm{G}}(d, \mathcal{R}) \leq d/2$. If d is odd, then the choice $|\mathcal{J}_1| = |\mathcal{J}_2| - 1 = (d-1)/2$ and $\kappa_i = 1$ for all $i = 1, \ldots, d$, except for one $i \in \mathcal{J}_2$ for which $\kappa_i = \min \mathcal{R}$, proves that $r_{\mathrm{G}}(d, \mathcal{R}) \leq (d + \min \mathcal{R})/2$. □

For the important cases of $\mathcal{R}$ introduced in (2) and (3), we can close the gap in (10).

Corollary 2: For $d \geq 1$ and $0 \leq \mu \leq 1$, it holds that

$$r_{\mathrm{G}}(d, \mathcal{R}_\mu) = \begin{cases} (1+\mu)(d+1)/4, & \text{if } d \equiv 1(2) \wedge \mu \\ & > (d-1)/(d+1) \\ d/2, & \text{otherwise.} \end{cases} \tag{11}$$

Proof: The result follows from Corollary 1 if d is even.

If d is odd and $\mu \leq (d-1)/(d+1)$, then the choice $|\mathcal{J}_1| = |\mathcal{J}_2| + 1 = (d+1)/2$ and $\kappa_i = (d-1)/(d+1)$ if $i \in \mathcal{J}_1$ and $\kappa_i = 1$ if $i \in \mathcal{J}_2$ in Theorem 1 shows that $r_{\mathrm{G}}(d, \mathcal{R}_\mu) \leq d/2$, and the result follows from Corollary 1.

Now, suppose that d is odd and $\mu > (d-1)/(d+1)$. The choice $|\mathcal{J}_1| = |\mathcal{J}_2| + 1 = (d+1)/2$ and $\kappa_i = \mu$ if $i \in \mathcal{J}_1$ and $\kappa_i = 1$ if $i \in \mathcal{J}_2$ in Theorem 1 shows that $r_{\mathrm{G}}(d, \mathcal{R}_\mu) \leq (1+\mu)(d+1)/4$. On the other hand, for any $\mathcal{J}_1$ and $\mathcal{J}_2$ in Theorem 1, such that $|\mathcal{J}_1| > |\mathcal{J}_2|$, we have

$$\sum_{i \in \mathcal{J}_1} \kappa_i - \sum_{i \in \mathcal{J}_2} \kappa_i \geq \mu |\mathcal{J}_1| - |\mathcal{J}_2| \geq \mu(d+1)/2 - (d-1)/2. \tag{12}$$

This proves that $r_{\mathrm{G}}(d, \mathcal{R}_\mu) \geq (1+\mu)(d+1)/4$. □

Corollary 3: For $d \geq 1$ and $m \in \{1, 2, 3, \ldots\}$, it holds that

$$r_{\mathrm{G}}(d, \mathcal{R}_m) = \begin{cases} d/2 + 1/(2m), & \text{if } d \equiv m \equiv 1(2) \\ d/2, & \text{otherwise.} \end{cases} \tag{13}$$

Proof: Since $\min \mathcal{R}_m$ is 0 if m is even and $1/m$ if m is odd, the result follows from Corollary 1 if d is even or m is even.

Now, let both m and d be odd. Then, from Corollary 1

$$d/2 \leq r_{\mathrm{G}}(d, \mathcal{R}_m) \leq d/2 + 1/(2m).$$

From the definition of $\mathcal{R}_m$, we know that for any $\mathcal{J}_1$ and $\mathcal{J}_2$ in Theorem 1 and any $\kappa_1, \ldots, \kappa_d \in \mathcal{R}_m$, the expression $|\sum_{i \in \mathcal{J}_1} \kappa_i - \sum_{i \in \mathcal{J}_2} \kappa_i|$ is an integer multiple of $1/m$. Hence, $r_{\mathrm{G}}(d, \mathcal{R}_m) < d/2 + 1/(2m)$ implies $r_{\mathrm{G}}(d, \mathcal{R}_m) = d/2$. In this case, Theorem 1 gives

$$\sum_{i \in \mathcal{J}_1} \kappa_i = \sum_{i \in \mathcal{J}_2} \kappa_i$$

for some disjoint sets $\mathcal{J}_1$ and $\mathcal{J}_2$ such that $\mathcal{J}_1 \cup \mathcal{J}_2 = \{1, 2, \ldots, d\}$ and some $\kappa_1, \ldots, \kappa_d \in \mathcal{R}_m$. Since all elements in $\mathcal{R}_m$ are odd multiples of $1/m$, it follows that $|\mathcal{J}_1|$ and $|\mathcal{J}_2|$ are either both even or both odd. This contradicts the fact that $|\mathcal{J}_1| + |\mathcal{J}_2| = d$, which is odd. □

III. Limited-Trial Decoding

As stated in Section I, limiting the maximum number of decoding trials to a number less than $\lceil d/2 \rceil$ leads to a computational complexity which is smaller than Forney's original algorithm. However, this may also lead to a degraded performance. In order to keep the loss in performance as small as possible, we have to come up with smart erasing strategies. Kovalev [12] has proposed fixed and optimized erasing strategies for the case $\mathcal{R} = [0, 1]$. Here, we will extend Kovalev's work to $\mathcal{R} \subset [0, 1]$ and include other erasing strategies as well.

Let the maximum number of trials be denoted by l and let the erasing strategy be denoted by $\mathcal{A}$. Such an erasing strategy $\mathcal{A}$ is, in fact, an algorithm which generates upon receipt of a sequence $\boldsymbol{\alpha}$ a set of nonnegative integers $\mathcal{I} = \{i_1, i_2, \ldots, i_l\}$. In the jth trial ($j = 1, 2, \ldots, l$), the i_j most unreliable symbols in $\boldsymbol{r}$ are erased before the received symbol sequence is fed into the (algebraic) error-erasure decoder. If this decoder generates a codeword $\boldsymbol{c}$ satisfying (6), then this codeword is taken as the final decoding result, else the next trial is performed, until the maximum number of trials has been reached. For Forney's algorithm, denoted by $\mathcal{A}^{\mathrm{F}}$, we have $l = \lceil d/2 \rceil$ and $i_j = 2j - 1$ (if d is even) or $i_j = 2j - 2$ (if d is odd).

For a given code $\mathcal{C}$ of Hamming distance d and length n, a given reliability set $\mathcal{R}$, and a given algorithm $\mathcal{A}$, let $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})$ denote the largest real number r for which the following assertion holds: for any transmitted codeword $\boldsymbol{c}$ from $\mathcal{C}$ and any received vector $\boldsymbol{r}$ of length n with reliability vector $\boldsymbol{\alpha} \in \mathcal{R}^n$ such that $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) < r$, the original codeword $\boldsymbol{c}$ is delivered by the decoder based on algorithm $\mathcal{A}$. Of course, $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})$, which is the *guaranteed error-correction radius achievable by the decoder*, does not exceed $r_{\mathrm{G}}(d, \mathcal{R})$. We also introduce the normalization of $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})$ with respect to $r_{\mathrm{G}}(d, \mathcal{R})$, i.e.,

$$\rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}) = \frac{r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})}{r_{\mathrm{G}}(d, \mathcal{R})} \tag{14}$$

which may be considered as the fraction of the code's guaranteed error-correction radius achievable by algorithm $\mathcal{A}$.

As the notation suggests, $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})$ may depend on the code $\mathcal{C}$ not only by its Hamming distance d. This will be illustrated by the following example. Let $\mathcal{R} = \mathcal{R}_3 = \{1/3, 1\}$ and let the single-trial algorithm $\mathcal{A}'$ be such that two most unreliable symbols are erased if $|\{i\colon \alpha_i = 1\}|$ is a multiple of 3 and that no symbols are erased otherwise. It can be easily shown that $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_3, \mathcal{A}') = 1$ if $\mathcal{C}$ is such that $n = d = 3$, while $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_3, \mathcal{A}') = r_{\mathrm{G}}(3, \mathcal{R}_3) = 5/3$ if $\mathcal{C}$ is such that $n = 5$ and $d = 3$.

In the next three sections, we will study the guaranteed error-correction radius achievable by fixed, threshold, and optimized erasing strategies, respectively. In order to facilitate the computations, we introduce for a code $\mathcal{C}$, a fixed reliability vector $\boldsymbol{\alpha}$, and an erasing set $\mathcal{I}$, the parameter $u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I})$, which is defined as the smallest real number u for which there exist a codeword $\boldsymbol{c} \in \mathcal{C}$, and a received sequence $\boldsymbol{r}$ with reliability sequence $\boldsymbol{\alpha}$, such that $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) = u$ and $\boldsymbol{c}$ is not generated in any decoding trial by the decoder based on $\mathcal{I}$. We have the following explicit expression for $u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I})$.

Lemma 1: For a code $\mathcal{C}$ of length n and Hamming distance d, a reliability vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, and an erasing set $\mathcal{I} = \{i_1, i_2, \ldots, i_l\}$ of size l, it holds that

$$u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) = n/2 - \sum_{i=1}^{n} \alpha_i/2 + \sum_{j=1}^{l} \sum_{i=i_j+1}^{i_j+b_j} \alpha_i \tag{15}$$

where

$$b_j = \max\left\{0, \left\lceil \left(d - i_j - 2\sum_{k=j+1}^{l} b_k\right) \Big/ 2 \right\rceil\right\}, \quad \text{for } j = l, l-1, \ldots, 1.$$

Proof: For a received sequence $\boldsymbol{r}$ with reliability sequence $\boldsymbol{\alpha}$, decoding trial j will generate a codeword $\boldsymbol{c}$ if and only if the number of erasures i_j and the number of nonerased errors $t_j = |\{i\colon i > i_j \wedge c_i \neq r_i\}|$ are such that $2t_j + i_j < d$. Hence, the smallest number of errors which results in not generating codeword $\boldsymbol{c}$ in trial j is thus $\max\{0, \lceil (d-i_j)/2 \rceil\}$. Further, note that the generalized distance $d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha})$ is minimum in case the erroneous positions are immediately following the erased positions. Applying this argument for $j = l, \ldots, 1$ subsequently concludes the proof. □

IV. Fixed Erasing

For reduced GMD decoding with fixed erasing, the erasing set $\mathcal{I}$ is fixed, i.e., it does not depend on $\boldsymbol{\alpha}$. Such an erasing strategy is denoted by $\mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}$. Note that erasing one extra symbol does not decrease the number of correctable errors in case the number of erasures and the Hamming distance are of the same parity [6], and that erasing d or more symbols does not make sense. Hence, we assume with regard to the set $\mathcal{I} = \{i_1, \ldots, i_l\}$ that $l \leq \lceil d/2 \rceil$, $-i_1 = i_0 \leq 0 \leq i_1 < \cdots < i_l < i_{l+1} = d+1$, and $d - i_j \equiv 1 (2)$ for all j. For such sets $\mathcal{I}$, we can write i_j $(j = 0, \ldots, l+1)$ in the format

$$i_j = d + 1 - 2a_j \tag{16}$$

where the a_j are integers such that

$$0 = a_{l+1} < a_l < \cdots < a_1 \leq a_0 = d + 1 - a_1.$$

We have the following result for $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}})$.

Theorem 2: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, a reliability set $\mathcal{R}$ with minimum μ, and an erasing set $\mathcal{I}$ of size l satisfying (16), it holds that

$$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}) = \min\left\{ r_{\mathrm{G}}(d, \mathcal{R}),\ \frac{d+1-\mu i_1}{2} + \frac{(\mu-1)}{4} \max_{k=0,\ldots,l} (i_{k+1} - i_k) \right\} \tag{17}$$

where $i_0 = -i_1$ and $i_{l+1} = d+1$.

Proof: From the definitions it follows that

$$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}) = \min\left\{ r_{\mathrm{G}}(d, \mathcal{R}),\ \min_{\boldsymbol{\alpha} \in \mathcal{R}^n} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) \right\}. \tag{18}$$

Observing $b_j = a_j - a_{j+1} = (i_{j+1} - i_j)/2$ for $j = 1, \ldots, l$, it follows from Lemma 1 that

$$u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) = n/2 - \sum_{j=1}^{l} \sum_{i=(i_{j-1}+i_j)/2+1}^{i_j} \alpha_i/2 + \sum_{j=1}^{l} \sum_{i=i_j+1}^{(i_j+i_{j+1})/2} \alpha_i/2 - \sum_{i=(i_l+i_{l+1})/2+1}^{n} \alpha_i/2. \tag{19}$$

Hence, $\min_{\boldsymbol{\alpha} \in \mathcal{R}^n} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I})$ is achieved for an $\boldsymbol{\alpha}$ with

$$\alpha_i = \theta_j \quad \text{if } (i_{j-1} + i_j)/2 + 1 \leq i \leq (i_j + i_{j+1})/2, \quad \text{for } 1 \leq j \leq l+1 \tag{20}$$

where $\mu = \theta_0 \leq \theta_1 \leq \cdots \leq \theta_{l+1} = 1$ and $i_{l+2} = 2n - d - 1$. For such an $\boldsymbol{\alpha}$ we have

$$u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) = \left(i_l + i_{l+1} + \sum_{j=1}^{l} \theta_j (i_{j-1} - 2i_j + i_{j+1}) \right) \Big/ 4. \tag{21}$$

Minimizing (21) over all possible sequences $\theta = (\theta_1, \ldots, \theta_l)$, we may assume that $\theta_j = \theta_{j-1}$ if $i_{j-1} - 2i_j + i_{j+1} > 0$, and $\theta_j = \theta_{j+1}$ otherwise $(j = 1, \ldots, l)$. Continuing this argument, it follows with $\theta_0 = \mu$ and $\theta_{l+1} = 1$, that the minimum in (21) over all θ is achieved for a θ satisfying $\theta_j = \mu$ if $1 \leq j \leq k$, and $\theta_j = 1$ if $k+1 \leq j \leq l$, where $k \in \{0, \ldots, l\}$. Substituting this θ into (21) gives for the $\boldsymbol{\alpha}$ derived from this θ by (20)

$$u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) = (2d + 2 - 2\mu i_1 + (\mu - 1)(i_{k+1} - i_k))/4. \tag{22}$$

Since $\mu - 1 \leq 0$, the expression in (22) is minimum if $i_{k+1} - i_k$ is maximum. With (18), this concludes the proof. □

Of particular interest among all sets $\mathcal{I}$ of a certain size l are the ones maximizing $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}})$. Switching to notation (16) and first assuming that a_1 is fixed, we choose $a_2, \ldots, a_l$ such that

$$a_j = \begin{cases} a_{j-1} - \lceil a_1/l \rceil, & \text{for } j = 2, \ldots, a_1 - l\lfloor a_1/l \rfloor + 1 \\ a_{j-1} - \lfloor a_1/l \rfloor, & \text{for } j = a_1 - l\lfloor a_1/l \rfloor + 2, \ldots, l \end{cases} \tag{23}$$

in order to maximize (17). Next, we maximize over all integers a_1 such that $l \leq a_1 \leq \lceil d/2 \rceil$, which results in

$$a_1 = \begin{cases} l \left\lceil \frac{d+1}{2l+1} \right\rceil, & \text{if } 0 \leq \mu \leq \frac{1}{2l+1} \\ & \quad \wedge \left\lceil \frac{d+1}{2l+1} \right\rceil \leq \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor \\ l \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor, & \text{if } \frac{1}{2l+1} < \mu < \frac{1}{2\lceil \frac{d}{2} \rceil - 2l \lfloor \lceil \frac{d}{2} \rceil / l \rfloor + 1} \\ & \quad \wedge \left\lceil \frac{d+1}{2l+1} \right\rceil \leq \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor \\ \lceil \frac{d}{2} \rceil & \text{otherwise.} \end{cases} \tag{24}$$

Together, (24), (23), and (16) provide a set $\mathcal{I}$ maximizing the guaranteed error-correction radius over all l-trial fixed erasing strategies in case $\mathcal{R}$ is a reliability set with minimum μ, which leads to the following results.

Corollary 4: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, a reliability set $\mathcal{R}$ with minimum μ, and $1 \leq l \leq \lceil d/2 \rceil$, it holds that

$$\max_{\mathcal{I}\colon |\mathcal{I}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}) = \begin{cases} \omega\left(l \left\lceil \frac{d+1}{2l+1} \right\rceil \right), & \text{if } 0 \leq \mu \leq \frac{1}{2l+1} \\ & \quad \wedge \left\lceil \frac{d+1}{2l+1} \right\rceil \leq \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor \\ \omega\left(l \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor \right), & \text{if } \frac{1}{2l+1} < \mu < \frac{1}{2\lceil \frac{d}{2} \rceil - 2l \lfloor \lceil \frac{d}{2} \rceil / l \rfloor + 1} \\ & \quad \wedge \left\lceil \frac{d+1}{2l+1} \right\rceil \leq \left\lfloor \lceil \frac{d}{2} \rceil / l \right\rfloor \\ \omega\left(\lceil \frac{d}{2} \rceil \right), & \text{otherwise} \end{cases} \tag{25}$$

where

$$\omega(x) = \min\{1, (2\mu x + (1-\mu)(d + 1 - \lceil x/l \rceil))/(2r_{\mathrm{G}}(d, \mathcal{R}))\}.$$

Corollary 5: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, a reliability set $\mathcal{R} \supseteq \{0, 1\}$, and $1 \leq l \leq \lceil d/2 \rceil$, it holds that

$$\max_{\mathcal{I}\colon |\mathcal{I}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}) = \lceil 2ld/(2l+1) \rceil / d. \tag{26}$$

Corollary 6: For a code $\mathcal{C}$ of Hamming distance approaching infinity, a reliability set $\mathcal{R}$ with minimum μ, and $1 \leq l \leq \lceil d/2 \rceil$, it holds that

$$\max_{\mathcal{I}\colon |\mathcal{I}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{I}}^{\mathrm{FE}}) = \begin{cases} 2l/(2l+1), & \text{if } \mu \leq 1/(2l+1) \\ (2l + \mu - 1)/(2l), & \text{if } \mu > 1/(2l+1). \end{cases} \tag{27}$$

The result from Corollary 6 is graphically represented in Fig. 1. Further, note from Corollary 4 that for any code $\mathcal{C}$ and any reliability set $\mathcal{R}$, Forney's erasing algorithm $\mathcal{A}^{\mathrm{F}}$ achieves the guaranteed error-correction radius, i.e., $\rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}^{\mathrm{F}}) = 1$.

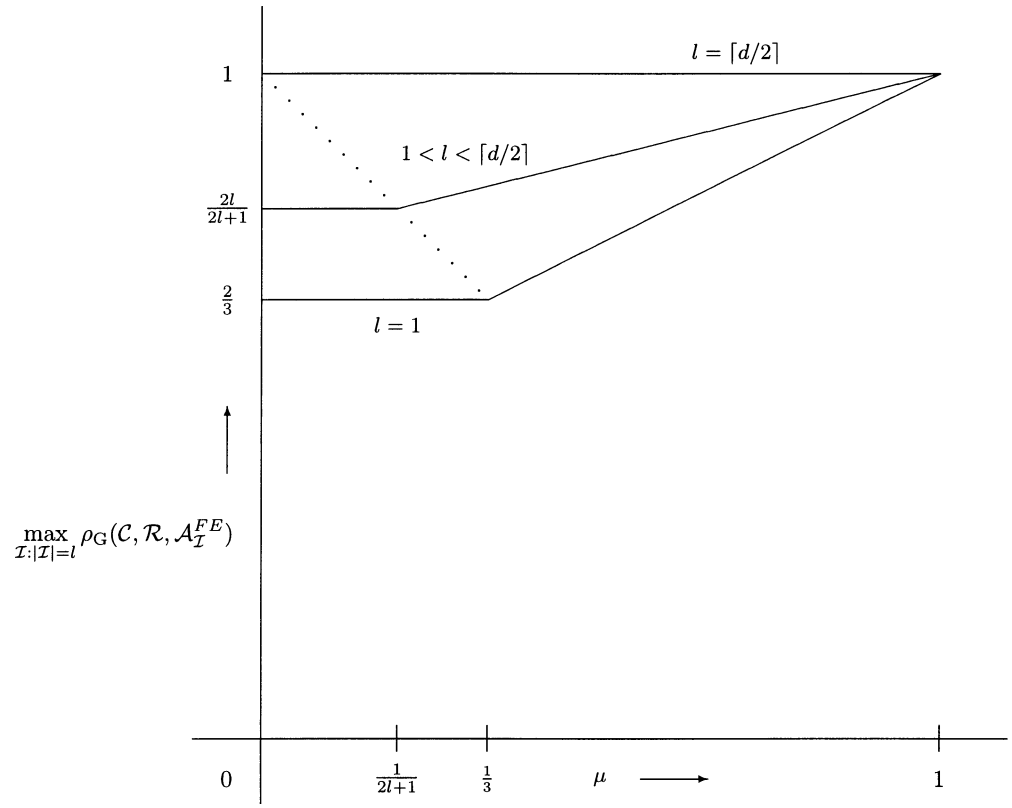

Fig. 1. Maximum normalized guaranteed error-correction radius for l-trial GMD decoding with fixed erasing and reliability set $\mathcal{R}$ with minimum μ, in the case of codes $\mathcal{C}$ of Hamming distance approaching infinity.

V. Threshold Erasing

For reduced GMD decoding with threshold erasing, the erasure patterns are determined by a threshold set $\mathcal{T} = \{\theta_1, \ldots, \theta_l\}$ with $\theta_j \in \mathcal{R}$ for all j. We assume $1 \le l \le |\mathcal{R}|$ and $\theta_1 < \cdots < \theta_l$. In the jth trial, all received symbols r_i for which $\alpha_i < \theta_j$ are erased. Such an erasing strategy is denoted by $\mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}$. An important benefit of threshold erasing is that there is no need to sort the received symbols according to their reliability values before erasing those with lowest reliability, which is the case for fixed erasing (and, thus, for Forney's algorithm).

We have the following result for $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}})$.

Theorem 3: For a code $\mathcal{C}$ of Hamming distance $d \ge 1$, reliability set $\mathcal{R}$, and threshold set $\mathcal{T} = \{\theta_1, \ldots, \theta_l\}$, it holds that

$$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \begin{cases} \frac{d}{2} - \frac{d}{4} \max_{t=0,\ldots,l} (\theta_{t+1}^{-} - \theta_t), & \text{if } d \equiv 0(2) \\ \min \left\{ r_{\mathrm{G}}(d, \mathcal{R}), \frac{d-\theta_1^{-}}{2} - \frac{d-1}{4} \right. & \\ \qquad \left. \cdot \max_{t=0,\ldots,l} (\theta_{t+1}^{-} - \theta_t) \right\}, & \text{if } d \equiv 1(2) \end{cases} \tag{28}$$

where $\theta_1^{-} = -\theta_1$ if $\theta_1 = \min \mathcal{R} = \mu$, $\theta_j^{-} = \sup\{\nu \in \mathcal{R}\colon \nu < \theta_j\}$ if $1 \le j \le l$ and $\theta_j > \mu$, $\theta_0 = -\theta_1^{-}$, and $\theta_{l+1}^{-} = 1$.

Proof: From the definitions it follows that

$$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \min \left\{ r_{\mathrm{G}}(d, \mathcal{R}), \min_{\mathcal{I}} \min_{\boldsymbol{\alpha}} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) \right\} \tag{29}$$

where the $\min_{\boldsymbol{\alpha}}$ operation is over all $\boldsymbol{\alpha} \in \mathcal{R}^n$ for which threshold set $\mathcal{T}$ applied on $\boldsymbol{\alpha}$ leads to a given erasing set $\mathcal{I} = \{i_1, \ldots, i_l\}$ with $0 = i_0 \le i_1 \le \cdots \le i_l \le i_{l+1} = n$, such that $i_1 = 0$ if $\theta_1 = \min \mathcal{R}$, and the $\min_{\mathcal{I}}$ operation is over all possible $\mathcal{I}$ of this kind. For given $\mathcal{I}$, the $\min_{\boldsymbol{\alpha}} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I})$ is achieved by the $\boldsymbol{\alpha}$ with

$$\alpha_i = \begin{cases} \theta_j^{-}, & \text{if } i_{j-1} + b_{j-1} + 1 \le i \le i_j, \text{ for } j = 1, \ldots, l+1 \\ \theta_j, & \text{if } i_j + 1 \le i \le i_j + b_j, \quad \text{for } j = 1, \ldots, l \end{cases} \tag{30}$$

where $b_0 = 0$ and

$$\begin{aligned} b_j &= \max \left\{ 0, \left\lceil \left(d - i_j - 2 \sum_{k=j+1}^{l} b_k \right) \Big/ 2 \right\rceil \right\} \\ &= \max\{0, \lceil (d - i_j)/2 \rceil - \max\{0, \lceil (d - i_{j+1})/2 \rceil\}\}, \\ &\qquad \text{for } j = l, l-1, \ldots, 1. \end{aligned}$$

Substituting (30) into (15) gives

$$\begin{aligned} & u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) \\ &= n/2 - \sum_{j=1}^{l} \sum_{i=i_{j-1}+b_{j-1}+1}^{i_j} \alpha_i/2 + \sum_{j=1}^{l} \sum_{i=i_j+1}^{i_j+b_j} \alpha_i/2 \\ &\quad - \sum_{i=i_l+b_l+1}^{n} \alpha_i/2 \\ &= n/2 - \sum_{j=1}^{l} \sum_{i=i_{j-1}+b_{j-1}+1}^{i_j} \theta_j^{-}/2 + \sum_{j=1}^{l} \sum_{i=i_j+1}^{i_j+b_j} \theta_j/2 \\ &\quad - \sum_{i=i_l+b_l+1}^{n} 1/2 \\ &= \frac{1}{2} \left(i_l + b_l - \sum_{j=1}^{l} \theta_j^{-} (i_j - i_{j-1} - b_{j-1}) + \sum_{j=1}^{l} b_j \theta_j \right) \\ &= \frac{1}{2} \sum_{j=1}^{l} ((\theta_{j+1}^{-} - \theta_j^{-}) i_j + (\theta_{j+1}^{-} + \theta_j) b_j) \\ &= \frac{1}{2} \sum_{j=1}^{l} \Big((\theta_{j+1}^{-} - \theta_j^{-}) i_j + (\theta_{j+1}^{-} - \theta_j^{-} + \theta_j - \theta_{j-1}) \\ &\qquad \cdot \max\{0, \lceil (d - i_j)/2 \rceil\} \Big). \end{aligned} \tag{31}$$

The minimum of (31) over all $\mathcal{I} = \{i_1, \ldots, i_l\}$ such that $0 = i_0 \leq i_1 \leq \cdots \leq i_l \leq i_{l+1} = n$ is attained by

$$i_j = \begin{cases} 0, & \text{if } (1 = j \leq t \wedge (d \equiv 0(2) \vee \theta_1 = \mu)) \\ & \quad \vee (2 \leq j \leq t \wedge d \equiv 0(2)) \\ 1, & \text{if } d \equiv 1(2) \wedge ((1 = j \leq t \wedge \theta_1 > \mu) \\ & \quad \vee 2 \leq j \leq t) \\ d, & \text{if } t+1 \leq j \leq l \end{cases} \tag{32}$$

for some integer t, where $0 \leq t \leq l$ if $\theta_1 > \mu$, and $1 \leq t \leq l$ if $\theta_1 = \mu$. Substituting (32) into (31), minimizing the resulting expression over t, while observing that $\theta_1^- - \theta_0 = -2\mu \leq 1 - \theta_l = \theta_{l+1}^- - \theta_l$ in case $\theta_1 = \mu$, and, finally, using (29), while noting that $r_{\mathrm{G}}(d, \mathcal{R}) \geq d/2$, concludes the proof. □

In case $l = |\mathcal{R}|$, we have $\mathcal{T} = \mathcal{R}$ and it follows immediately from Theorem 3 that $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{R}}^{\mathrm{TE}}) = r_{\mathrm{G}}(d, \mathcal{R})$, i.e., $\rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{R}}^{\mathrm{TE}}) = 1$. Of particular interest among all sets $\mathcal{T}$ of a certain size $l < |\mathcal{R}|$ are the ones maximizing $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}})$. Next, we determine such threshold sets for the reliability sets from (2) and (3).

First, we consider the case $\mathcal{R} = \mathcal{R}_\mu$ with $\mu \in [0, 1]$. For fixed $\theta_1 \in [\mu, 1]$, minimization of

$$\max_{t=1,\ldots,l} (\theta_{t+1}^- - \theta_t) = \max_{t=1,\ldots,l} (\theta_{t+1} - \theta_t) \tag{33}$$

where we define $\theta_{l+1} = 1$, is achieved by choosing

$$\theta_j = 1 - (l + 1 - j)(1 - \theta_1)/l, \qquad \text{for } 2 \leq j \leq l. \tag{34}$$

Substituting this into (28), the resulting expression is maximized by the choice

$$\theta_1 = \begin{cases} \frac{1}{2l+1}, & \text{if } \left(d \equiv 0(2) \wedge \mu \leq \frac{1}{2l+1}\right) \\ & \quad \vee \left(d \equiv 1(2) \wedge \mu \leq \frac{d-1-2l}{(2l+1)(d-1+2l)}\right) \\ \mu, & \text{otherwise.} \end{cases} \tag{35}$$

Together, (34) and (35) determine an optimal l-trial threshold erasing procedure in case $\mathcal{R} = \mathcal{R}_\mu$, which brings us to the following results.

Corollary 7: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, $\mu \in [0, 1]$, and $l \geq 1$, it holds that

$$\max_{\mathcal{T}:|\mathcal{T}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_\mu, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \begin{cases} \frac{2l+\mu-1}{2l}, & \text{if } d \equiv 0(2) \wedge \mu > \frac{1}{2l+1} \\ \frac{(d+2l-1)\mu+2ld-d+1}{2ld}, & \text{if } d \equiv 1(2) \wedge \frac{d-2l-1}{(2l+1)(d+2l-1)} \\ & \quad < \mu < \frac{d-1}{d+2l-1} \\ 1, & \text{if } d \equiv 1(2) \wedge \mu \geq \frac{d-1}{d+2l-1} \\ \frac{2l}{2l+1}, & \text{otherwise.} \end{cases} \tag{36}$$

Corollary 8: For a code $\mathcal{C}$ of Hamming distance approaching infinity, $\mu \in [0, 1]$, and $l \geq 1$, it holds that

$$\max_{\mathcal{T}:|\mathcal{T}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_\mu, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \begin{cases} 2l/(2l+1), & \text{if } \mu \leq 1/(2l+1) \\ (2l+\mu-1)/(2l), & \text{if } \mu > 1/(2l+1). \end{cases} \tag{37}$$

Note the resemblance of the results presented in Corollaries 6 and 8, but be aware of the fact that the former holds for any set $\mathcal{R}$ with minimum μ, while the latter explicitly assumes $\mathcal{R} = \mathcal{R}_\mu = [\mu, 1]$.

Next, we consider the case $\mathcal{R} = \mathcal{R}_m$ with $m \in \{1, 2, 3, \ldots\}$. For fixed

$$\theta_1 = 1 - 2(i-1)/m \tag{38}$$

with $l \leq i \leq \lfloor m/2 \rfloor + 1$, minimization of

$$\max_{t=1,\ldots,l} (\theta_{t+1}^- - \theta_t) = \max_{t=1,\ldots,l} (\theta_{t+1} - \theta_t - 2/m) \tag{39}$$

where we define $\theta_{l+1} = 1 + 2/m$, is achieved by choosing

$$\theta_j = \begin{cases} \theta_{j-1} + 2\lfloor i/l \rfloor/m, & \text{for } 2 \leq j \leq l + l\lfloor i/l \rfloor - i \\ \theta_{j-1} + 2\lceil i/l \rceil/m, & \text{for } l + l\lfloor i/l \rfloor - i + 1 \leq j \leq l. \end{cases} \tag{40}$$

Substituting (38) and (40) into (28), we find that the resulting expression is maximum when

$$i = \begin{cases} \left\lceil \frac{l(m+1)}{2l+1} \right\rceil, & \text{if } d \equiv 0(2) \\ l \left\lceil \frac{m+1}{2l+1} \right\rceil, & \text{if } d \equiv 1(2) \wedge \left\lceil \frac{m+1}{2l+1} \right\rceil \leq \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor \wedge d \geq 2l+1 \\ l \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor, & \text{if } d \equiv 1(2) \wedge \left\lceil \frac{m+1}{2l+1} \right\rceil \leq \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor \\ & \quad \wedge 2\lceil m/2 \rceil - 2l \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor + 1 < d \leq 2l \\ m/2 + 1, & \text{if } d \equiv 1(2) \wedge m \equiv 0(2) \wedge l = m/2 + 1 \\ \lceil m/2 \rceil, & \text{otherwise.} \end{cases} \tag{41}$$

Together (38), (40), and (41) determine an optimal l-trial threshold erasing procedure in case $\mathcal{R} = \mathcal{R}_m$, which brings us to the following results.

Corollary 9: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, $m \in \{1, 2, 3, \ldots\}$, and $1 \leq l \leq \lfloor m/2 \rfloor + 1$, it holds that

$$\max_{\mathcal{T}:|\mathcal{T}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_m, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \begin{cases} \frac{1}{m} \left\lceil \frac{2lm}{2l+1} \right\rceil, & \text{if } d \equiv 0(2), \\ \phi\left(l \left\lceil \frac{m+1}{2l+1} \right\rceil\right), & \text{if } d \equiv 1(2) \wedge \left\lceil \frac{m+1}{2l+1} \right\rceil \leq \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor \\ & \quad \wedge d \geq 2l+1, \\ \phi\left(l \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor\right), & \text{if } d \equiv 1(2) \wedge \left\lceil \frac{m+1}{2l+1} \right\rceil \leq \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor \\ & \quad \wedge 2\lceil m/2 \rceil - 2l \left\lfloor \frac{\lceil m/2 \rceil}{l} \right\rfloor + 1 \\ & \quad < d \leq 2l, \\ \phi(\lceil m/2 \rceil) & \text{otherwise} \end{cases} \tag{42}$$

where

$$\phi(x) = \frac{2x + (d-1)(m + 1 - \lceil x/l \rceil)}{2m r_{\mathrm{G}}(d, \mathcal{R}_m)}. \tag{43}$$

Corollary 10: For a code $\mathcal{C}$ of Hamming distance approaching infinity, $m \in \{1, 2, 3, \ldots\}$, and $1 \leq l \leq \lfloor m/2 \rfloor + 1$, it holds that

$$\max_{\mathcal{T}:|\mathcal{T}|=l} \rho_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_m, \mathcal{A}_{\mathcal{T}}^{\mathrm{TE}}) = \lceil 2lm/(2l+1) \rceil/m. \tag{44}$$

VI. Optimized Erasing

For reduced GMD decoding with optimized erasing, the erasing set $\mathcal{I}$ is chosen based on the received reliability vector $\boldsymbol{\alpha}$, such that the achievable guaranteed error-correction radius by the decoder is maximum. Such an erasing strategy is denoted by $\mathcal{A}_l^{\mathrm{OE}}$, where l is the maximum number of trials. As for fixed erasing, we may assume with regard to the set $\mathcal{I} = \{i_1, \ldots, i_l\}$ that $l \leq \lceil d/2 \rceil$, $0 \leq i_1 < \cdots < i_l \leq d$, and $d - i_j \equiv 1(2)$ for all j. Note that

$$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_l^{\mathrm{OE}}) = \min \left\{ r_{\mathrm{G}}(d, \mathcal{R}), \min_{\boldsymbol{\alpha} \in \mathcal{R}^n} \max_{\mathcal{I}:|\mathcal{I}|=l} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}, \mathcal{I}) \right\}. \tag{45}$$

For the reliability set $\mathcal{R} = [0, 1]$, Kovalev [12] has derived the following (nearly) tight bounds on $r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A}_l^{\mathrm{OE}})$.

TABLE I
DATA CONCERNING THE $\mathcal{A}_1^{\mathrm{OE}}$ ALGORITHM IN CASE OF A RELIABILITY SET $\mathcal{R} = \mathcal{R}_\mu$ WITH $\mu \in [0,\ 1]$ AND A CODE $\mathcal{C}$ WITH HAMMING DISTANCE $d \geq 1$

μ, d	$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_\mu, \mathcal{A}_1^{\mathrm{OE}})$
$0 \leq \mu \leq 1 \wedge d = 1$	$(1+\mu)/2$
$0 \leq \mu < 1/2 \wedge d \equiv 0(2)$	$(3d+2)/8$
$1/2 \leq \mu \leq 1 \wedge d \equiv 0(2)$	$(d(1+\mu)+2(1-\mu))/4$
$0 \leq \mu < 1/2 \wedge d \equiv 3(4)$	$3(d+1)/8$
$0 \leq \mu < 1/3 \wedge d \geq 5 \wedge d \equiv 1(4)$	$(9d+7)/24$
$1/3 \leq \mu < 1/2 \wedge d \geq 5 \wedge d \equiv 1(4)$	$(3d+1+4\mu)/8$
$1/2 \leq \mu \leq 1 \wedge d \geq 3 \wedge d \equiv 1(2)$	$(d+1)(1+\mu)/4$

μ, d	$\boldsymbol{\alpha}^*$
$0 \leq \mu \leq 1 \wedge d = 1$	$(\mu, \mathbf{1})$
$0 \leq \mu < 1/2 \wedge d \equiv 0(2)$	$((1/2)^{d/2+1}, \mathbf{1})$
$1/2 \leq \mu \leq 1 \wedge d \equiv 0(2)$	$(\mu^{d/2+1}, \mathbf{1})$
$0 \leq \mu < 1/2 \wedge d \equiv 3(4)$	$((1/2)^{(d+1)/2}, \mathbf{1})$
$0 \leq \mu < 1/3 \wedge d \geq 5 \wedge d \equiv 1(4)$	$((1/3)^{(d+1)/2}, (2/3)^{(d-1)/4}, \mathbf{1})$
$1/3 \leq \mu < 1/2 \wedge d \geq 5 \wedge d \equiv 1(4)$	$(\mu^{(d+1)/2}, (2\mu)^{(d-1)/4}, \mathbf{1})$
$1/2 \leq \mu \leq 1 \wedge d \geq 3 \wedge d \equiv 1(2)$	$(\mu^{(d+1)/2}, \mathbf{1})$

μ, d	$\mathcal{S}$
$0 \leq \mu \leq 1 \wedge d = 1$	$\{0\}$
$0 \leq \mu \leq 1 \wedge d \equiv 0(4)$	$\{1, d/2+1\}$
$0 \leq \mu \leq 1 \wedge d \equiv 2(4)$	$\{1, d/2\}$
$0 \leq \mu < 1/2 \wedge d \equiv 3(4)$	$\{0, (d+1)/2\}$
$0 \leq \mu < 1/3 \wedge d \geq 5 \wedge d \equiv 1(4)$	$\{0, 2, (d-1)/2, (d+3)/2\}$
$1/3 \leq \mu < 1/2 \wedge d \geq 5 \wedge d \equiv 1(4)$	$\{0, (d-1)/2\}$
$1/2 \leq \mu \leq 1 \wedge d \geq 3 \wedge d \equiv 1(2)$	$\{0\}$

Index: ψ^y denotes the vector $(\psi, \psi, \ldots, \psi)$ of length y, and $\mathbf{1}$ is an all-one vector such that the length of $\boldsymbol{\alpha}^*$ equals n.

Theorem 4 (Kovalev): For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, and $1 \leq l \leq \lceil d/2 \rceil$, it holds that

$$(d+1-\lceil (d+1)/4l \rceil)/2 \leq r_{\mathrm{G}}(\mathcal{C},\ [0,\ 1],\ \mathcal{A}_l^{\mathrm{OE}}) < (d+2-\lceil (d+1)/4l \rceil)/2 \tag{46}$$

where equality holds in the first inequality in case $d+1$ is a multiple of $4l$.

Proof: The proof can be found in [12]. □

Since $r_{\mathrm{G}}(\mathcal{C},\ [0,\ 1],\ \mathcal{A}_l^{\mathrm{OE}}) \leq r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R},\ \mathcal{A}_l^{\mathrm{OE}})$ for any $\mathcal{R}$, the following result emerges from Theorem 4.

Corollary 11: For a code $\mathcal{C}$ of Hamming distance $d \geq 1$, a reliability set $\mathcal{R}$, and $1 \leq l \leq \lceil d/2 \rceil$, it holds that

$$r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R},\ \mathcal{A}_l^{\mathrm{OE}}) \geq (d+1-\lceil (d+1)/4l \rceil)/2. \tag{47}$$

For single-trial decoding with optimized erasing, we have the following results for the reliability sets from (2) and (3).

Theorem 5: For $\mu \in [0,\ 1]$ and a code $\mathcal{C}$ of Hamming distance $d \geq 1$, it holds that $r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_\mu,\ \mathcal{A}_1^{\mathrm{OE}})$ is as given in Table I.

Corollary 12: For $\mu \in [0,\ 1]$ and a code $\mathcal{C}$ of Hamming distance approaching infinity, it holds that

$$\rho_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_\mu,\ \mathcal{A}_1^{\mathrm{OE}}) = \begin{cases} 3/4 & \text{if } 0 \leq \mu \leq 1/2, \\ (1+\mu)/2 & \text{if } 1/2 < \mu \leq 1. \end{cases} \tag{48}$$

Theorem 6: For $m \geq 1$ and a code $\mathcal{C}$ of Hamming distance $d \geq 1$, it holds that $r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_m,\ \mathcal{A}_1^{OE})$ is as given in Table II.

Corollary 13: For $m \geq 1$ and a code $\mathcal{C}$ of Hamming distance approaching infinity, it holds that

$$\rho_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_m,\ \mathcal{A}_1^{\mathrm{OE}}) = \begin{cases} 1, & \text{if } m = 1,\ 2 \\ 7/9, & \text{if } m = 3 \\ 4/5, & \text{if } m = 5 \\ 3/4, & \text{if } m = 4 \text{ or } m \geq 6. \end{cases} \tag{49}$$

The proofs of Theorems 5 and 6 are extremely lengthy because of the many subcases which need to be considered. Therefore, we take the approach of first discussing one example case in detail, and then giving guidelines along which the proofs can be obtained in the remaining cases.

As an example, we consider the case $d,\ m \equiv 0(4)$. Let

$$\boldsymbol{\alpha}^* = \left((1/2)^{d/2+1},\ 1^{n-d/2-1}\right) \tag{50}$$

where ψ^y denotes the vector $(\psi,\ \psi,\ \ldots,\ \psi)$ of length y. From (15), we have

$$u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha}^*,\ \{i_1\}) = \begin{cases} (3d+2)/8, & \text{if } 1 \leq i_1 \leq d/2+1 \wedge i_1 \equiv 1(2) \\ (5d+6-4i_1)/8, & \text{if } d/2+3 \leq i_1 \leq d-1 \wedge i_1 \equiv 1(2) \end{cases} \tag{51}$$

and, thus, it follows from (45) that

$$r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_m,\ \mathcal{A}_1^{\mathrm{OE}}) \leq (3d+2)/8. \tag{52}$$

Now suppose that $r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_m,\ \mathcal{A}_1^{\mathrm{OE}}) < (3d+2)/8$, i.e., there exists an $\boldsymbol{\alpha} \in (\mathcal{R}_m)^n$ such that

$$u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha},\ \{i_1\}) \leq (3d+2)/8 - 1/m \tag{53}$$

for all odd i_1 such that $1 \leq i_1 \leq d-1$. Thus,

$$\begin{aligned}(3d+2)/4 - 2/m &\geq u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha},\ \{1\}) + u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha},\ \{d/2+1\}) \\ &= n - \alpha_1 - \sum_{i=3d/4+2}^{n} \alpha_i \geq 3d/4 + 1 - \alpha_1 \end{aligned} \tag{54}$$

which implies that $\alpha_i \geq \alpha_1 \geq 1/2 + 2/m$ for all $i = 1,\ \ldots,\ n$. Hence,

$$\begin{aligned} u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha},\ \{1\}) &= n/2 - \sum_{i=1}^{n} \alpha_i/2 + \sum_{i=2}^{d/2+1} \alpha_i \\ &\geq (d+2)/4 - \alpha_1/2 + \alpha_2/2 + \sum_{i=3}^{d/2+1} \alpha_i/2 \\ &\geq (3d+2)/8 \end{aligned} \tag{55}$$

contradicting (53). Hence, equality holds in (52). In conclusion

$$r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_m,\ \mathcal{A}_1^{\mathrm{OE}}) = (3d+2)/8 \tag{56}$$

in case $d,\ m \equiv 0(4)$, and a single-trial erasing strategy to achieve this is to choose the erasing set $\mathcal{I} = \{i_1\}$ such that

$$i_1 = \begin{cases} 1, & \text{if } \sum_{i=2}^{d/2+1} \alpha_i \geq \sum_{i=d/2+2}^{3d/4+1} \alpha_i \\ d/2+1, & \text{otherwise.} \end{cases} \tag{57}$$

Other cases can be proved similarly using the following guidelines. In Tables I and II, we provide for all cases a vector $\boldsymbol{\alpha}^* \in \mathcal{R}^n$ and a set $\mathcal{S}$, for which it can be shown that for any $\boldsymbol{\alpha} \in \mathcal{R}^n$ there exists an $i_1 \in \mathcal{S}$ such that

$$u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha},\ \{i_1\}) \geq \max_{0 \leq j \leq n} u_{\mathrm{G}}(\mathcal{C},\ \boldsymbol{\alpha}^*,\ \{j\}).$$

TABLE II
DATA CONCERNING THE $\mathcal{A}_1^{\mathrm{OE}}$ ALGORITHM IN CASE OF A RELIABILITY SET $\mathcal{R} = \mathcal{R}_m$ WITH $m \in \{1, 2, 3, \ldots\}$ AND A CODE $\mathcal{C}$ WITH HAMMING DISTANCE $d \geq 1$

m, d	$r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_m, \mathcal{A}_1^{\mathrm{OE}})$
$m \leq 2 \vee d \leq 2$	$\lceil md/2 \rceil / m$
$m = 3 \wedge d \geq 3$	$(d + \lfloor d/3 \rfloor - \lfloor d/6 \rfloor + 1)/3$
$m = 5 \wedge d \geq 3$	$(3d + 1 - 2\lfloor d/2 \rfloor)/5$
$m \geq 4 \wedge m \neq 5 \wedge d \equiv 3(4)$	$\lceil 3(d+1)m/8 \rceil / m$
$m \geq 4 \wedge m \neq 5 \wedge d = 4$	$(\lceil 3m/2 \rceil + \lceil (m-1)/4 \rceil)/m$
$m \geq 4 \wedge m \neq 5 \wedge d \equiv 0(4) \wedge d \geq 5$	$(\lceil 3md/8 \rceil + \lceil m/4 \rceil)/m$
$m \equiv 0(2) \wedge m \geq 4 \wedge d \equiv 1(8) \wedge d \geq 5$	$((3d+5)m/8 - \lfloor m/3 \rfloor)/m$
$m \equiv 1(2) \wedge m \geq 7 \wedge d \equiv 1(8) \wedge d \geq 5$	$((3d+5)m/8 - \lceil m/3 \rceil + 1)/m$
$m \geq 4 \wedge m \neq 5 \wedge d \equiv 5(8) \wedge d \geq 5$	$(\lceil (3d+5)m/8 \rceil - \lfloor m/3 \rfloor)/m$
$m \geq 4 \wedge m \neq 5, 9 \wedge d \equiv 2(4) \wedge d \geq 5$	$\lceil (3d+2)m/8 \rceil / m$
$m = 9 \wedge d \equiv 2(4) \wedge d \geq 5$	$(\lfloor 9(3d+2)/8 \rfloor + 1)/9$

m, d	$\boldsymbol{\alpha}^*$
$m \leq 2 \vee d \leq 2$	$((1 - 2\lfloor m/2 \rfloor / m)^d, \mathbf{1})$
$m = 3 \wedge d \geq 3$	$((1/3)^{\lfloor d/2 \rfloor + \lfloor d/3 \rfloor - \lfloor d/6 \rfloor + 1}, \mathbf{1})$
$4 \leq m \leq 5 \wedge d \geq 3$	$((1 - 2/m)^{\lfloor d/2 \rfloor + 1}, \mathbf{1})$
$m \geq 6 \wedge d \equiv 1(4) \wedge d \geq 3$	$(\lambda_1^{(d+1)/2}, \lambda_2^{\lceil (d-1)/8 \rceil}, \lambda_3^{\lfloor (d-1)/8 \rfloor}, \mathbf{1})$
$m \geq 6 \wedge m \equiv 0(4) \wedge d \not\equiv 1(4) \wedge d \geq 3$	$(1/2)^{\lfloor d/2 \rfloor + 1}, \mathbf{1})$
$m \geq 6 \wedge m \equiv 1(4) \wedge d \not\equiv 1(4) \wedge d \geq 3 \wedge d \neq 4$	$(\lambda_4^{\lfloor d/2 \rfloor + 1}, \lambda_5^{\lfloor (d+5)/8 \rfloor}, \lambda_6^{\lfloor (d+1)/8 \rfloor}, \mathbf{1})$
$m \geq 6 \wedge m \equiv 1(4) \wedge d = 4$	$(((m+1)/(2m))^3, \mathbf{1})$
$m \geq 6 \wedge m \equiv 2(4) \wedge d \not\equiv 1(4) \wedge d \geq 3$	$(\lambda_4^{\lfloor d/2 \rfloor + 1}, \lambda_6^{\lfloor (d+1)/4 \rfloor}, \mathbf{1})$
$m \geq 6 \wedge m \equiv 3(4) \wedge d \not\equiv 1(4) \wedge d \geq 3$	$(\lambda_4^{\lfloor d/2 \rfloor + 1}, \lambda_6^{\lfloor (d+2)/8 \rfloor}, \mathbf{1})$

m, d	$\mathcal{S}$
$m = 1, 2 \wedge d \geq 1$	$\{y_1\}$
$m = 3 \wedge d \geq 1$	$\{0, 1, y_2 - 2, y_2 - 1, y_2, y_2 + 1\}$
$m = 5 \wedge d \geq 1$	$\{0, 1, y_3 - 1, y_3, y_3 + 1\}$
$m \neq 1, 2, 3, 5 \wedge d \equiv 0(4)$	$\{1, d/2 + 1\}$
$m \neq 1, 2, 3, 5 \wedge d \equiv 1(4)$	$\{0, 2, (d-1)/2, (d+3)/2\}$
$m \neq 1, 2, 3, 5, 9 \wedge d \equiv 2(4)$	$\{1, d/2\}$
$m = 9 \wedge d \equiv 2(4)$	$\{1, 3, d/2, d/2 + 2\}$
$m \neq 1, 2, 3, 5 \wedge d \equiv 3(4)$	$\{0, (d+1)/2\}$

Index: see Table I, plus $\lambda_1 = 1 - 2\lfloor m/3 \rfloor / m$, $\lambda_2 = 1 - 2(2\lfloor m/3 \rfloor - \lfloor m/2 \rfloor)/m$, $\lambda_3 = 1 - 2(2\lfloor m/3 \rfloor - \lceil m/2 \rceil)/m$, $\lambda_4 = 1 - 2\lceil m/4 \rceil / m$, $\lambda_5 = 1 - 4/m$, $\lambda_6 = 1 - 2/m$, $y_1 = |\{i : \alpha_i = 0\}|$, $y_2 = |\{i : \alpha_i = 1/3\}|$, and $y_3 = |\{i : \alpha_i = 1/5\}|$.

Since

$$\max_{0 \leq j \leq n} u_{\mathrm{G}}(\mathcal{C}, \boldsymbol{\alpha}^*, \{j\}) \leq r_{\mathrm{G}}(d, \mathcal{R})$$

in all cases, Theorems 5 and 6 then follow from (45).

It is to be expected that in deriving the achievable guaranteed error-correction radius for multitrial optimized erasing even more subcases need to be distinguished. This is not elaborated here, and we leave the matter at the important Kovalev bounds from Theorem 4 and Corollary 11. These bounds show that, for any code $\mathcal{C}$ and any reliability set $\mathcal{R}$, an error-correction radius of $d/2$ can be achieved in at most $\lceil (d+1)/4 \rceil$ trials with optimized erasing.

VII. ASYMPTOTIC PERFORMANCE ANALYSIS

Next, we study the performance of reduced GMD decoders in terms of the probability of unsuccessful decoding. Throughout this section, we assume that $\mathcal{C}$ is a binary linear code and that the code bits c_i are sent as antipodal signals (i.e., either a given waveform of energy E or its negative) over an AWGN channel (with two-sided spectral density $N_0/2$) with matched-filter reception. For convenience, define

$$\gamma = E/N_0. \tag{58}$$

The output z_i is a Gaussian random variable which has, under a convenient normalization, mean $\pm\gamma$ and variance $\gamma/2$, where the sign depends on whether a 0 or a 1 was transmitted. We let the sign of z_i decide whether r_i is 0 or 1, and assign a reliability value $\alpha_i \in \mathcal{R}$ according to the log-likelihood ratio. Details on this assignment are provided in the Appendix.

With regard to the decoder we assume it is a reduced GMD decoder with reliability set $\mathcal{R}$, erasing algorithm $\mathcal{A}$, and acceptance criterion (6). For ML decoding at high SNR, the probability of unsuccessful decoding is essentially $e^{-d\gamma}$ [7]. We are interested in the *asymptotic loss* of reduced GMD decoding compared to ML decoding, i.e., the extra power required to achieve the same probability of unsuccessful decoding as for ML decoding at SNR approaching infinity ($\gamma \to \infty$).

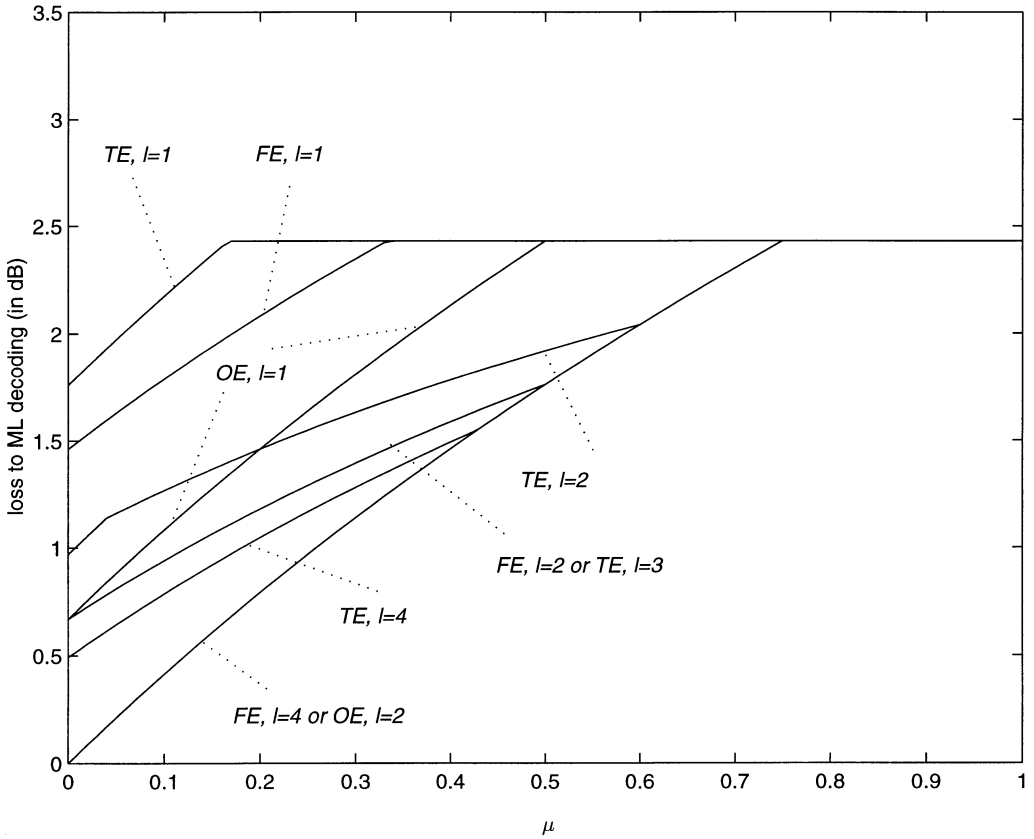

Fig. 2. Performance results for reduced GMD decoders, in case of binary antipodal signals, AWGN channel, SNR approaching infinity, codes of Hamming distance $d = 7$, reliability sets $\mathcal{R}_\mu$ with $\mu \in [0,\ 1]$, and l-trial decoding strategies with fixed erasing (FE), threshold erasing (TE), or optimized erasing (OE).

Theorem 7: For a reduced GMD decoder with erasing algorithm $\mathcal{A}$ and reliability set $\mathcal{R}_v$ with $v \in [0,\ 1] \cup \{1,\ 2,\ 3,\ \ldots\}$, operating on a code $\mathcal{C}$ of Hamming distance $d \geq 1$, the probability of unsuccessful decoding is essentially $e^{-2\gamma\sigma_v r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_v,\ \mathcal{A})}$ as $\gamma \to \infty$, and, thus, the asymptotic loss (in decibels) is

$$10\log_{10}(1/\sigma_v) + 10\log_{10}(d/(2r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_v,\ \mathcal{A}))) \tag{59}$$

where

$$\sigma_v = \begin{cases} 1/(v+1), & \text{for } v \in [0,\ 1] \\ v/(v+1), & \text{for } v \in \{1,\ 3,\ 5,\ \ldots\} \\ 2v\left(v+1-\sqrt{v^2+2v}\right), & \text{for } v \in \{2,\ 4,\ 6,\ \ldots\}. \end{cases} \tag{60}$$

Proof: See the Appendix. □

Note that for GMD decoding ($v = 0$, $\mathcal{A} = \mathcal{A}^{\mathrm{F}}$) both terms in (59) are zero, so at high SNR, GMD decoding performs as well as ML decoding, which was the main conclusion from [6]. Hence, (59) can also be regarded as the asymptotic loss for reduced GMD decoding compared to GMD decoding. The first term in (59) depends only on the reliability set $\mathcal{R}$ and is called the *quantization loss*, since it is caused by the less accurate representation of the reliability information from the channel due to using only a subset $\mathcal{R}$ of $[0,\ 1]$ rather than $[0,\ 1]$ itself as in GMD decoding. The second term in (59) depends on the code $\mathcal{C}$, the reliability set $\mathcal{R}$, and the erasing algorithm $\mathcal{A}$. It is called the *radius loss*, since it is caused by the deviation of the guaranteed error-correction radius $r_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_v,\ \mathcal{A})$ compared to the radius $d/2$ for GMD decoding. Note that the radius loss is negative if the guaranteed error-correction radius exceeds $d/2$, in which case we actually have a radius gain.

Forney [6], [7] considered in particular the cases of errors-only decoding ($v = 1$), error-erasure decoding ($v = 2$), and GMD decoding ($v = 0$ or $v \to \infty$), all with $\mathcal{A} = \mathcal{A}^{\mathrm{F}}$, for which he found asymptotic losses to ML decoding of 3.01, 1.63, and 0 dB, respectively. There are indications, however, that the actual asymptotic loss for errors-only decoding ($v = 1$) is dependent on the code distance d. For example, for the trivial case $d = 1$ (no coding), it can easily be argued that GMD does not lead to a lower probability of unsuccessful decoding than errors-only decoding, which suggests that for small d the gain of GMD decoding over errors-only decoding could be less than 3.01 dB. Also, the probability of unsuccessful decoding $e^{-d\gamma}$ for ML (and thus GMD) decoding decreases when increasing an odd code distance $d = 2t+1$ by one to $d = 2t+2$, while in errors-only decoding the performance is actually equal for these two distances, i.e., the loss for $d = 2t+1$ should be smaller than for $d = 2t+2$. These observations can be explained by the notions of quantization and radius loss. For $v = 1$ the quantization loss is $10\log_{10} 2 = 3.01$ dB, which indeed equals Forney's result. On the other hand, the radius loss is 0 dB if d is even, and $10\log_{10}(d/(d+1))$ decibels if d is odd. Hence, the total loss is $10\log_{10} 2 = 3.01$ dB if d is even, and $10\log_{10}(2d/(d+1)) < 10\log_{10} 2 = 3.01$ dB if d is odd.

Further numerical illustrations of (59) are provided in Figs. 2–5. The results are obtained by substituting results from Sections IV–VI on the achievable guaranteed error-correction radius into (59). In each figure, the best, i.e., lowest, possible curve is achieved by erasing algorithms $\mathcal{A}$ with $\rho_{\mathrm{G}}(\mathcal{C},\ \mathcal{R},\ \mathcal{A}) = 1$, e.g., by Forney's $\lceil d/2 \rceil$-trial fixed erasing or by $|\mathcal{R}|$-trial threshold erasing. In case the code's Hamming distance d approaches infinity, $\rho_{\mathrm{G}}(\mathcal{C},\ \mathcal{R},\ \mathcal{A}^{\mathrm{OE}}_{\lceil (d+1)/4 \rceil}) = 1$, and so the lowest curves in Figs. 4 and 5 are also achieved by $\lceil (d+1)/4 \rceil$-trial optimized erasing. In case $d = 7$ and $\mu \in [0,\ 1]$, $\rho_{\mathrm{G}}(\mathcal{C},\ \mathcal{R}_\mu,\ \mathcal{A}^{\mathrm{OE}}_2) = 1$, which follows from Corollaries 11 and 2 if $\mu \in [0,\ 3/4]$ and from Theorem 5 and Corollary 2 otherwise. Hence, the lowest curve in Fig. 2 is also achieved by double-trial optimized erasing.

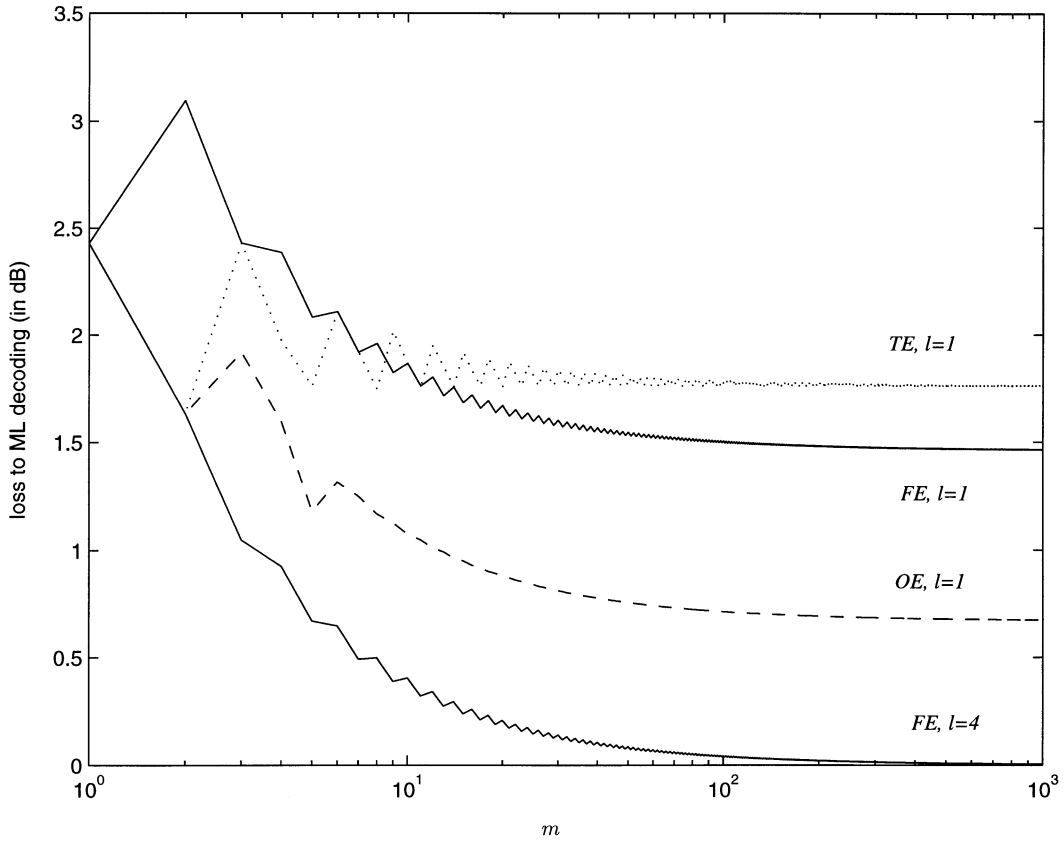

Fig. 3. Performance results for reduced GMD decoders, in case of binary antipodal signals, AWGN channel, SNR approaching infinity, codes of Hamming distance $d = 7$, reliability sets $\mathcal{R}_m$ with $m \in \{1, 2, 3 \ldots\}$, and l-trial decoding strategies with fixed erasing (FE: solid lines), threshold erasing (TE: dotted line), or optimized erasing (OE: dashed line).

The lowest curves in Figs. 4 and 5 represent the quantization loss, which depends only on the reliability set $\mathcal{R}$. The difference between the quantization loss curve and the curve associated with a certain erasing algorithm represents the radius loss due to the limited-trial strategy. Note that for codes with an odd Hamming distance, e.g., 7 as for the famous binary Golay code, the radius loss may be negative. This may result in curves as given in Figs. 2 and 3, which are (partly) below the quantization loss curves from Figs. 4 and 5, respectively.

The figures show that significant complexity reduction is possible at the price of only a modest performance loss. For example, for codes of Hamming distance approaching infinity, it follows from the dotted curve in Fig. 5 that we are within 1 dB from ML decoding, by performing at most $l = 2 \ (\ll \lceil d/2 \rceil)$ decoding trials with threshold erasing (and in particular without requiring the ordering of reliability symbols) and using only the three reliability levels 0, $1/2$, and 1 from $\mathcal{R}_4$.

Figs. 3 and 5 reveal an interesting phenomenon. Notice that the overall loss is not necessarily a nonincreasing function of m. This points to the rather surprising observation that a finer quantization of the reliability set does not necessarily lead to a better performance. The reason is that the radius loss may increase by an amount greater than the reduction in the quantization loss as the number of quantization levels increases. As an example, we consider codes of Hamming distance approaching infinity, a reliability set $\mathcal{R}_m$, and a fixed erasing single-trial decoder (see upper solid curve in Fig. 5). If $m = 2$, i.e., $\mathcal{R} = \mathcal{R}_2 = \{0, 1\}$, the quantization loss is 1.63 dB and the radius loss is 1.76 dB, which gives a total loss of 3.40 dB. If we do not use reliability value 0, i.e., we assign reliability value 1 to all received symbols and thus have an effective reliability set $\mathcal{R} = \mathcal{R}_1 = \{1\}$, the quantization loss increases to 3.01 dB. But since there is no radius loss in this case, the total loss is only 3.01 dB, which is less than 3.40 dB. The radius loss increases by allowing symbols to have reliability value 0 since the generalized distance between the transmitted codeword and the received vector increases if, among the symbols with reliability value 0, there are more correct symbols than incorrect ones. If this generalized distance exceeds the guaranteed error-correction radius, the decoder fails to recover the transmitted codeword. Finally, also note from Fig. 5 that $\mathcal{R}_3$ gives a loss of 3.01 dB as well, but here it consists of a quantization loss of 1.25 dB and a radius loss of 1.76 dB.

VIII. Application to Concatenated Coding

We now apply the concept of reduced GMD decoding to concatenated coding schemes [7], [16], similarly to the approach from [3]. We consider a scheme with a linear q-ary outer code $\mathcal{C}_{\text{outer}}$ of length n and Hamming distance d, and a linear inner code $\mathcal{C}_{\text{inner}}$ of length n_{in}, size (at least) q, and Hamming distance m. The code symbols c_i from an outer codeword $\boldsymbol{c}$ are encoded according to $\mathcal{C}_{\text{inner}}$ into inner codewords x_i, which are transmitted and then received as z_i. Each z_i is a sequence of n_{in} symbols from the inner code alphabet. Next, the (bounded distance) inner decoder looks for an inner codeword which is at Hamming distance at most $\lfloor (m-1)/2 \rfloor$ from z_i. If it succeeds in finding such an inner codeword w_i, then it outputs the symbol r_i (from the outer code alphabet) associated with w_i according to $\mathcal{C}_{\text{inner}}$ with reliability $\alpha_i = 1 - 2d_{\text{H}}(z_i, w_i)/m$, otherwise, it chooses an arbitrary inner codeword w_i and outputs the symbol r_i associated with this codeword with reliability $\alpha_i = 0$. Hence, $\mathcal{R} = \mathcal{R}_m$ if m is even or the inner code is perfect, and $\mathcal{R} = \mathcal{R}_m \cup \{0\}$ otherwise.

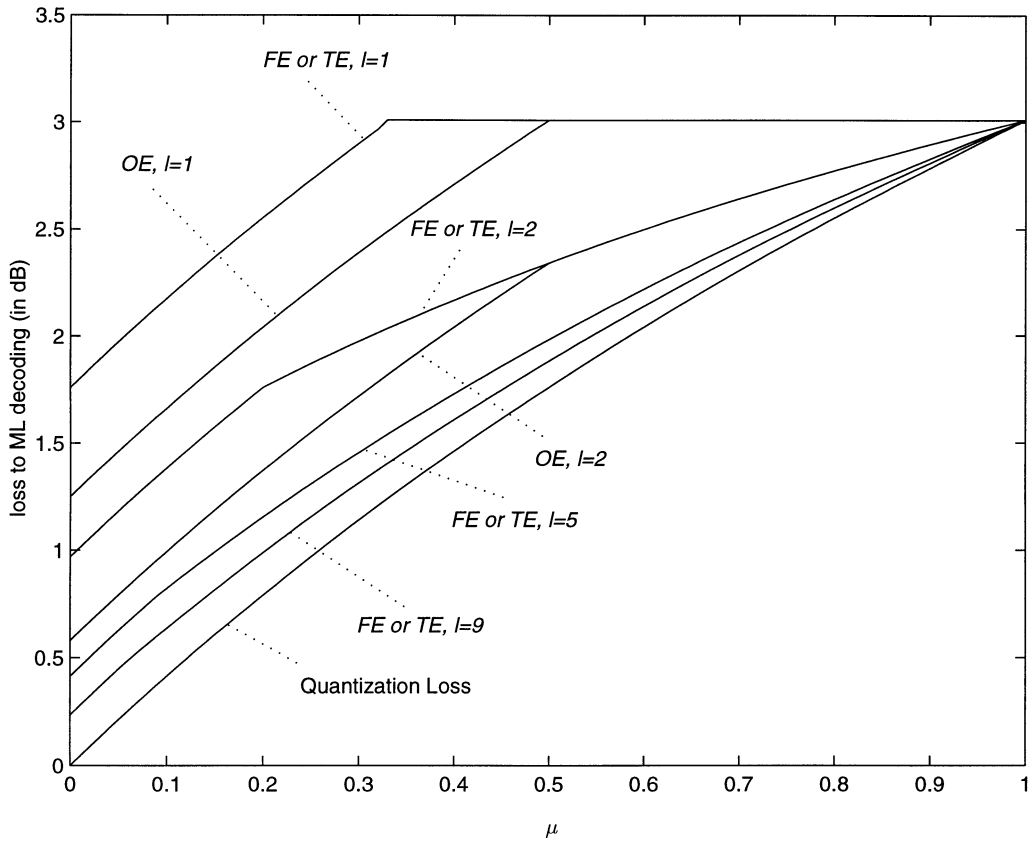

Fig. 4. Performance results for reduced GMD decoders, in case of binary antipodal signals, AWGN channel, SNR approaching infinity, codes of Hamming distance approaching infinity, reliability sets $\mathcal{R}_\mu$ with $\mu \in [0, 1]$, and l-trial decoding strategies with fixed erasing (FE), threshold erasing (TE), or optimized erasing (OE).

Finally, the vectors $\boldsymbol{r}$ and $\boldsymbol{\alpha}$ are processed by a reduced GMD decoder based on an erasing algorithm $\mathcal{A}$, as considered earlier in this correspondence.

Let $e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A})$ denote the smallest number of channel errors for which a decoding error or failure may occur in such a concatenated coding scheme. Hence, the maximum number of errors for which correction is guaranteed is $e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A}) - 1$. The following result relates $e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A})$ to the guaranteed error-correction radius.

Theorem 8: For an inner code $\mathcal{C}_{\text{inner}}$ of Hamming distance $m \geq 1$, an outer code $\mathcal{C}_{\text{outer}}$, and an erasing strategy $\mathcal{A}$, we have

$$m \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_m \cup \{0\}, \mathcal{A}) \leq e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A}) \leq m \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_m, \mathcal{A}) \quad (61)$$

where equality holds in the last inequality if at least one of the following conditions holds:

2) m is even;
3) $\mathcal{C}_{\text{inner}}$ is perfect;
4) $\mathcal{A}$ is of fixed, threshold, or optimized type.

Proof:

A) Let $r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_m, \mathcal{A})$ be achieved by a codeword $\boldsymbol{c}$ from $\mathcal{C}_{\text{outer}}$ and a received vector $\boldsymbol{r}$ with reliability vector $\boldsymbol{\alpha} \in (\mathcal{R}_m)^n$. Thus, for these $\boldsymbol{c}$, $\boldsymbol{r}$, and $\boldsymbol{\alpha}$, $d_{\text{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) = r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_m, \mathcal{A})$ and the GMD decoder based on erasing strategy $\mathcal{A}$ with input $\boldsymbol{r}$ and $\boldsymbol{\alpha}$ delivers either no codeword or a codeword $\hat{\boldsymbol{c}} \neq \boldsymbol{c}$. For the concatenated coding scheme, we may assume that $d_H(x_i, w_i) = m$ if $r_i \neq c_i$. Hence, α_i can be obtained by $m(1 - \alpha_i)/2$ errors during transmission of x_i if $r_i = c_i$, and by $m(1 + \alpha_i)/2$ transmission errors if $r_i \neq c_i$. Hence,

$$\begin{aligned} &e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A}) \\ &\quad \leq \sum_{i: r_i = c_i} m(1 - \alpha_i)/2 + \sum_{i: r_i \neq c_i} m(1 + \alpha_i)/2 \\ &\quad = m \times d_{\text{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) = m \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_m, \mathcal{A}) \end{aligned} \quad (62)$$

which shows the second inequality in (61).

B) Let $e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A})$ be achieved by an inner codeword sequence $\boldsymbol{x} = (x_1, \ldots, x_n)$, associated to (outer) codeword $\boldsymbol{c}$, and a received vector sequence $\boldsymbol{z} = (z_1, \ldots, z_n)$, leading to vectors $\boldsymbol{r}$ and $\boldsymbol{\alpha}$. Thus, for these $\boldsymbol{x}$, $\boldsymbol{z}$, $\boldsymbol{c}$, $\boldsymbol{r}$, and $\boldsymbol{\alpha}$, $\sum_{i=1}^{n} d_{\text{H}}(x_i, z_i) = e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A})$ and the GMD decoder based on erasing strategy $\mathcal{A}$ with input $\boldsymbol{r}$ and $\boldsymbol{\alpha}$ delivers either no codeword or a codeword $\hat{\boldsymbol{c}} \neq \boldsymbol{c}$. Hence,

$$\begin{aligned} &e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A}) \\ &\quad = \sum_{i=1}^{n} d_{\text{H}}(x_i, z_i) \\ &\quad \geq \sum_{i: x_i = w_i} d_{\text{H}}(z_i, w_i) + \sum_{i: x_i \neq w_i} (m - d_{\text{H}}(z_i, w_i)) \\ &\quad \geq \sum_{i: r_i = c_i} m(1 - \alpha_i)/2 + \sum_{i: r_i \neq c_i} m(1 + \alpha_i)/2 \\ &\quad = m \times d_{\text{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha}) \geq m \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}^*, \mathcal{A}) \end{aligned} \quad (63)$$

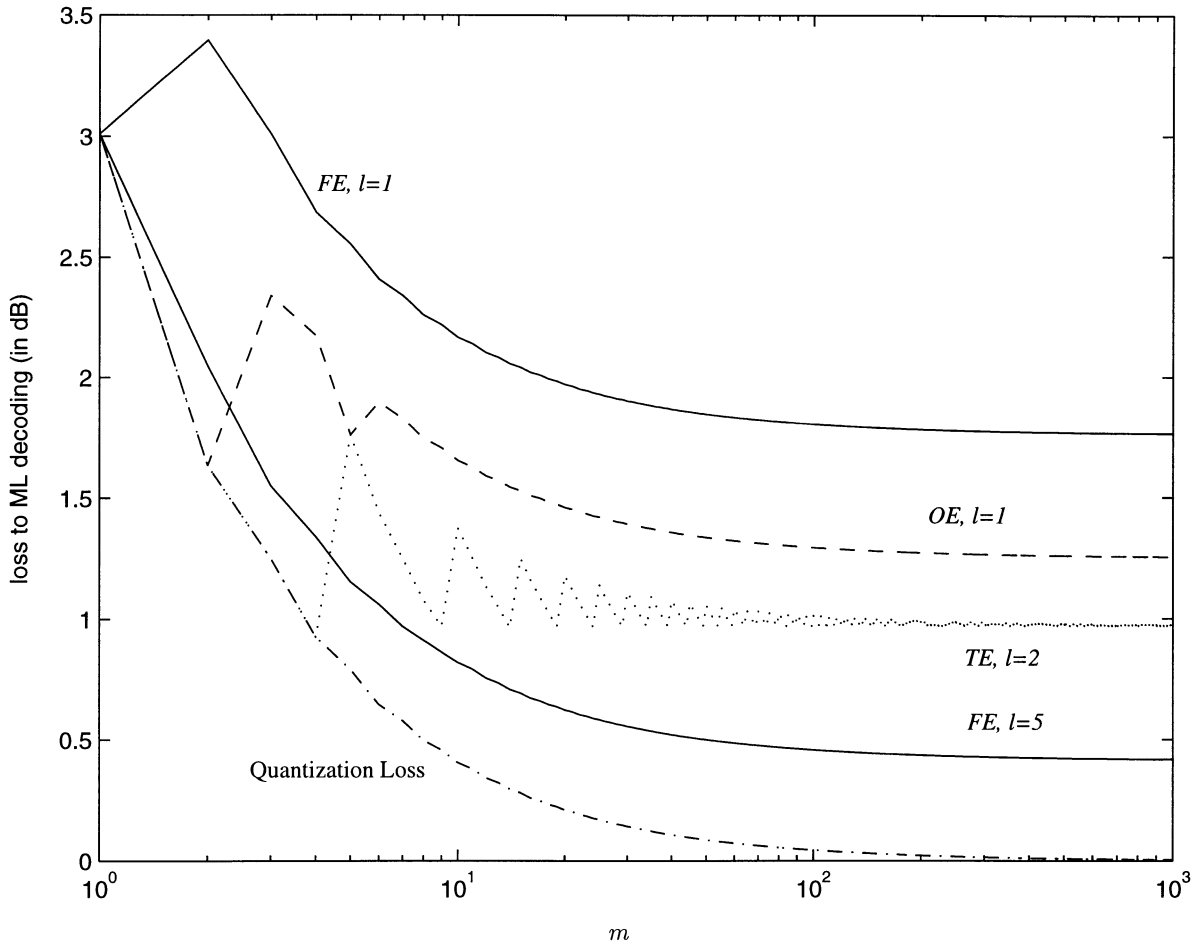

Fig. 5. Performance results for reduced GMD decoders, in case of binary antipodal signals, AWGN channel, SNR approaching infinity, codes of Hamming distance approaching infinity, reliability sets $\mathcal{R}_m$ with $m \in \{1, 2, 3, \ldots\}$, and l-trial decoding strategies with fixed erasing (FE: solid lines), threshold erasing (TE: dotted line), or optimized erasing (OE: dashed line).

where w_i is the inner codeword associated with symbol r_i and $\mathcal{R}^* = \cup_{i=1}^{n}\{\alpha_i\}$. Since $\mathcal{R}^* \subseteq \mathcal{R}_m \cup \{0\}$ and thus

$$r_{\mathrm{G}}(\mathcal{C}_{\mathrm{outer}}, \mathcal{R}^*, \mathcal{A}) \geq r_{\mathrm{G}}(\mathcal{C}_{\mathrm{outer}}, \mathcal{R}_m \cup \{0\}, \mathcal{A})$$

the first inequality in (61) follows.

C) Next, we show that equality holds in the second inequality in (61) if at least one of the three mentioned conditions holds.

C1) If m is even, then $\mathcal{R}_m \cup \{0\} = \mathcal{R}_m$, and the result follows immediately from (61).

C2) If $\mathcal{C}_{\mathrm{inner}}$ is perfect, then $\mathcal{R}^* \subseteq \mathcal{R}_m$, and the result follows from (62) and (63) since

$$r_{\mathrm{G}}(\mathcal{C}_{\mathrm{outer}}, \mathcal{R}^*, \mathcal{A}) \geq r_{\mathrm{G}}(\mathcal{C}_{\mathrm{outer}}, \mathcal{R}_m, \mathcal{A}).$$

C3) Finally, we consider the case that the erasing algorithm $\mathcal{A}$ is of fixed, threshold, or optimized type. We assume m is odd. Suppose that for the vector $\boldsymbol{\alpha}$ in Part B of this proof, the set $\mathcal{Z} = \{i\colon \alpha_i = 0\}$ is nonempty. For all $i \in \mathcal{Z}$, $d_{\mathrm{H}}(x_i, z_i) \geq (m+1)/2$, and thus there exists a $\tilde{\boldsymbol{z}} = (\tilde{z}_1, \ldots, \tilde{z}_n)$, leading to vectors $\tilde{\boldsymbol{r}}$ and $\tilde{\boldsymbol{\alpha}}$, such that $\tilde{z}_i = z_i$ (and, thus, $\tilde{r}_i = r_i$ and $\tilde{\alpha}_i = \alpha_i$) for all $i \notin \mathcal{Z}$, and $d_{\mathrm{H}}(x_i, \tilde{z}_i) = (m+1)/2$, $\tilde{r}_i \neq c_i$, and $\tilde{\alpha}_i = 1/m$ for all $i \in \mathcal{Z}$. In trial j, let the numbers of erased symbols in $\boldsymbol{r}$ and $\tilde{\boldsymbol{r}}$ be e_j and $\tilde{e}_j$, respectively, and let the numbers of nonerased incorrect symbols in $\boldsymbol{r}$ and $\tilde{\boldsymbol{r}}$ be t_j and $\tilde{t}_j$, respectively. We now show that for the erasing strategies under consideration, trial j being not successful for $\boldsymbol{r}$ implies it is not successful for $\tilde{\boldsymbol{r}}$ as well.

fixed erasing: $\tilde{e}_j = e_j$ and $\tilde{t}_j \geq t_j$, and thus,

$$2\tilde{t}_j + \tilde{e}_j \geq 2t_j + e_j \geq d;$$

threshold erasing: $\tilde{e}_j \leq e_j$ and $\tilde{t}_j = t_j + e_j - \tilde{e}_j$, and thus,

$$2\tilde{t}_j + \tilde{e}_j = 2t_j + 2e_j - \tilde{e}_j \geq 2t_j + e_j \geq d;$$

optimized erasing: suppose that trial j, with input $\tilde{\boldsymbol{r}}$ and $\tilde{\boldsymbol{\alpha}}$ would result in the original codeword $\boldsymbol{c}$; then adapt the algorithm such that in case of reliability vector $\boldsymbol{\alpha}$, $\tilde{e}_j$ symbols are erased in the jth trial rather than e_j; for the modified algorithm, trial j, with input $\boldsymbol{r}$ and $\boldsymbol{\alpha}$, would result in the original codeword $\boldsymbol{c}$.

If (at least) one of the l trials generates for $\boldsymbol{r}$ with $\boldsymbol{\alpha}$ the original codeword $\boldsymbol{c}$ but decoding is still unsuccessful since the acceptance criterion is not met, then it will also not be met for $\tilde{\boldsymbol{r}}$ and $\tilde{\boldsymbol{\alpha}}$, since $d_{\mathrm{G}}(\boldsymbol{c}, \tilde{\boldsymbol{r}}, \tilde{\boldsymbol{\alpha}}) \geq d_{\mathrm{G}}(\boldsymbol{c}, \boldsymbol{r}, \boldsymbol{\alpha})$. Noting that

$$\sum_{i=1}^{n} d_{\mathrm{H}}(x_i, \tilde{z}_i) \leq \sum_{i=1}^{n} d_{\mathrm{H}}(x_i, z_i) = e(\mathcal{C}_{\mathrm{outer}}, \mathcal{C}_{\mathrm{inner}}, \mathcal{A})$$

we thus conclude that we may assume $\alpha_i > 0$ for all i, i.e., $\mathcal{R}^* \subseteq \mathcal{R}_m$, and the result follows once again from (62) and (63). □

Since it follows from Theorem 8 that

$$e(\mathcal{C}_{\mathrm{outer}}, \mathcal{C}_{\mathrm{inner}}, \mathcal{A}) = m \times r_{\mathrm{G}}(\mathcal{C}_{\mathrm{outer}}, \mathcal{R}_m, \mathcal{A}) \qquad (64)$$

holds for a very broad range of cases, one might conjecture that it holds for any case. However, the following example shows that this is not true. Let $\mathcal{C}_{\text{inner}}$ be a nonperfect code of Hamming distance $m = 3$ and let $\mathcal{C}_{\text{outer}}$ be a code of Hamming distance $d = 3$. Further, let the single-trial erasing rule $\mathcal{A}^*$ be such that all n received symbols are erased if at least one received reliability value equals 0, and that no received symbols are erased otherwise. It is easy to see that $e(\mathcal{C}_{\text{outer}}, \mathcal{C}_{\text{inner}}, \mathcal{A}^*) = 2$, since two channel errors may lead to a received symbol of reliability 0 and thus to a decoding failure. However,

$$3 \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_3, \mathcal{A}^*) = 3 \times r_{\text{G}}(\mathcal{C}_{\text{outer}}, \mathcal{R}_3, \mathcal{A}^{\text{FE}}_{\{0\}}) = 3 \times 4/3 = 4.$$

Hence, (64) does not hold for this example.

IX. Discussion

In this correspondence, we present a framework for reduced GMD decoding. In particular, our work covers various reliability sets, various erasing strategies, and various maximum numbers of decoding trials. Many results scattered in the literature and many new results are presented and derived in this general setting. Limiting the number of allowable reliability values and the maximum number of trials may considerably decrease the complexity of the detector and the decoder, but possibly at the expense of performance degradation. Our goal is to study the efficiency of reduced GMD decoding schemes.

In comparing fixed and threshold erasing, notice that for large values of d, the results on asymptotic performance derived in Section VII tend to favor threshold erasing over fixed erasing where the reliability values ranging from 0 to 1 are quantized into the $\lfloor m/2 \rfloor + 1$ levels of $\mathcal{R}_m$. As mentioned before, $l = 2$ decoding trials with threshold erasing based on the reliability set $\mathcal{R}_m$, with $m = 4$, suffice to achieve asymptotic performance within 1 dB of that of ML decoding. If fixed erasing is used instead, the number of trials l and/or the size of the reliability set $\lfloor m/2 \rfloor + 1$ need to be much larger in order to guarantee the same performance based on our results. In particular, if $l = 2$ trials are used, then $m = 140$ guarantees less than 1-dB asymptotic loss compared to ML decoding, while if $m = 4$, then $l = 29$. More attractive choices for l and m in this case are $(l, m) = (3, 13), (4, 9), (5, 7)$,(6, 6), and $(9, 5)$.

By definition, optimal erasing maximizes the guaranteed error-correction radius achievable by the decoder. Although the numbers of symbols to be erased in the different trials depends on the reliability vector $\boldsymbol{\alpha}$, in all cases investigated, there is a surprisingly very small number of possibilities that need to be considered. As an example, for a code of Hamming distance d and for the reliability set $\mathcal{R}_m$, if $d,\ m \equiv 0(4)$, then an optimized erasing single-trial decoder erases i_1 least reliable symbols where i_1 is one of two possible values given in (57). More generally, looking at the sizes of $\mathcal{S}$ in Tables I and II, which gives the different possibilities for the number of symbols to be erased in single-trial decoding in the cases $\mathcal{R} = \mathcal{R}_\mu$ and $\mathcal{R} = \mathcal{R}_m$, shows that the number of possibilities is typically one or two, and never exceeds six. This interesting observation even holds for multitrial decoders. Indeed, if $d + 1$ is a multiple of $4l$, then there are just two possibilities that need to be considered for the numbers of symbols to be erased in the l trials regardless of the value of l [12].

A glance at the results of Sections IV–VI reveals that our success in determining the guaranteed error-correction radius achievable by a decoder depends very much on the erasing strategy. In Section IV, we succeed in determining the maximum guaranteed error-correction radius of an l-trial decoder employing fixed erasure for any l and any reliability set $\mathcal{R}$. In Section V, we determine this maximum radius if the decoder uses threshold erasing for any l but only in the cases $\mathcal{R} = \mathcal{R}_\mu$ or $\mathcal{R} = \mathcal{R}_m$. On the other hand, for optimal erasing, Section VI presents only bounds on the guaranteed error-correction radius achievable by an l-trial decoder and gives exact results only in the cases $l = 1$ and $\mathcal{R}$ is either $\mathcal{R}_\mu$ or $\mathcal{R}_m$.

Finally, note that the performance analysis as presented in Section VII is asymptotic. Therefore, it may not reflect well the decoder behavior at low- or medium-SNR values, especially for relatively long codes.

Appendix

In this appendix, we extend the performance analysis from [6], [7] for errors-only, error-erasure, and GMD decoding to reduced GMD decoding as considered in this correspondence. The setting has been described in the introductory paragraphs of Section VII. The analysis eventually leads to the proof of Theorem 7.

For simplicity, let the channel output z_i be denoted by just z. Based on z, a detector generates a binary symbol $r(z)$ and a reliability value $\alpha(z) \in \mathcal{R}$, which serve as inputs r_i and α_i to the decoder, respectively. Let $p_c(z)$ be the probability that the channel output is z and $r(z)$ is correct, and $p_e(z)$ be the probability that the channel output is z and $r(z)$ is not correct. Let y be the random variable which for a transmitted symbol takes on the value $(1-\alpha(z))$ if $r(z)$ is correct, and takes on the value $(1+\alpha(z))$ if $r(z)$ is incorrect. The moment-generating function of y is

$$g(s) = \overline{e^{sy}} = \int_z \left(p_c(z) e^{s(1-\alpha(z))} + p_e(z) e^{s(1+\alpha(z))} \right) dz. \quad (65)$$

Correct decoding of a transmitted codeword is guaranteed if the sum of n of these random variables is less than $b = 2r_{\text{G}}(\mathcal{C}, \mathcal{R}, \mathcal{A})$. Applying the (exponentially tight [11]) Chernoff bound, the probability P of unsuccessful decoding is upper-bounded by

$$P \le e^{-sb + n \ln g(s)} \quad (66)$$

for any $s \ge 0$. Hence, to obtain the tightest bound, we should minimize the exponent

$$X = -sb + n \ln g(s) \quad (67)$$

in (66). Note that for $s = 0$ we only obtain the trivial bound $P \le 1$, so we may further assume $s > 0$.

In order to find an assignment $\alpha(z)$ such that $g(s)$ is minimal, we equate the partial derivative of $p_c(z)e^{s(1-\alpha(z))} + p_e(z)e^{s(1+\alpha(z))}$ with respect to $\alpha(z)$ to zero. This gives

$$\alpha(z) = \frac{L(z)}{2s} \quad (68)$$

as the optimal assignment, where $L(z)$ is the log-likelihood ratio, i.e.,

$$L(z) = \ln \frac{p_c(z)}{p_e(z)}. \quad (69)$$

In case $L(z)/2s \notin \mathcal{R}$, the best thing to do is rounding off to a nearest value in $\mathcal{R}$. Hence, for $\mathcal{R}_\mu$ (with $\mu \in [0, 1]$) we have

$$\alpha_\mu(z) = \begin{cases} \mu, & \text{if } L(z) \le 2\mu s \\ \frac{L(z)}{2s}, & \text{if } 2\mu s < L(z) \le 2s \\ 1, & \text{if } L(z) > 2s \end{cases} \quad (70)$$

and for $\mathcal{R}_m$ (with $m = 1, 2, 3, \ldots$) we have

$$\alpha_m(z) = 1 - 2i/m, \quad \text{if } l_{i+1} \le L(z) < l_i \quad (71)$$

with $i = 0, 1, \ldots, \lfloor m/2 \rfloor$ and where

$$l_0 = \infty, \quad l_i = 2s(1-(2i-1)/m), \quad \text{for } 1 \le i \le \lfloor m/2 \rfloor,\ l_{\lfloor m/2 \rfloor}+1 = -\infty. \tag{72}$$

Hence, from (65) and (70), we find that the minimal $g(s)$ in case $\mathcal{R} = \mathcal{R}_\mu$ reads

$$\begin{aligned} g_\mu(s) = &\int_{z:\, L(z)\le 2\mu s} \left(p_c(z)e^{s(1-\mu)} + p_e(z)e^{s(1+\mu)}\right) dz \\ &+ \int_{z:\, 2\mu s < L(z) \le 2s} 2e^s \sqrt{p_c(z)p_e(z)}\, dz \\ &+ \int_{z:\, L(z) > 2s} (p_c(z) + p_e(z)e^{2s})\, dz \end{aligned} \tag{73}$$

and from (65) and (71), we find that the minimal $g(s)$ in case $\mathcal{R} = \mathcal{R}_m$ reads

$$\begin{aligned} g_m(s) = \sum_{i=0}^{\lfloor m/2 \rfloor} \int_{z:\, l_{i+1} \le L(z) < l_i} &\cdot \left(p_c(z)e^{2si/m} + p_e(z)e^{2s(1-i/m)}\right) dz. \end{aligned} \tag{74}$$

Since the sign of z decides whether $r(z)$ is 0 or 1, it follows that

$$p_c(z) = \frac{1}{2\sqrt{\pi\gamma}}\, e^{-(|z|-\gamma)^2/\gamma} \tag{75}$$

and

$$p_e(z) = \frac{1}{2\sqrt{\pi\gamma}}\, e^{-(|z|+\gamma)^2/\gamma} \tag{76}$$

which give

$$L(z) = 4|z|. \tag{77}$$

Hence, by substituting (75), (76), and (77) into (73) and (74), we obtain

$$\begin{aligned} g_\mu(s) = &e^{s(1-\mu)} \left(Q(-\xi) - Q\left(\frac{\mu s}{\xi} - \xi\right)\right) \\ &+ e^{s(1+\mu)} \left(Q(\xi) - Q\left(\frac{\mu s}{\xi} + \xi\right)\right) \\ &+ 2e^{s-\gamma} \left(Q\left(\frac{\mu s}{\xi}\right) - Q\left(\frac{s}{\xi}\right)\right) \\ &+ Q\left(\frac{s}{\xi} - \xi\right) + e^{2s} Q\left(\frac{s}{\xi} + \xi\right) \end{aligned} \tag{78}$$

and

$$\begin{aligned} g_m(s) = \sum_{i=1}^{\lfloor m/2 \rfloor} &\left(Q\left(\frac{l_i}{2\xi} + \xi\right) e^{2s(1-i/m)}(e^{2s/m} - 1)\right. \\ &\left. + Q\left(\frac{l_i}{2\xi} - \xi\right) e^{2si/m}(e^{-2s/m} - 1)\right) \\ &+ (1 - Q(\xi))e^{2s\lfloor m/2 \rfloor/m} + Q(\xi)e^{2s(1-\lfloor m/2 \rfloor/m)} \end{aligned} \tag{79}$$

where $\xi = \sqrt{2\gamma}$ and

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}}\, e^{-\lambda^2/2}\, d\lambda \tag{80}$$

which can be approximated for large x based on

$$Q(x) = \frac{e^{-x^2/2}}{x\sqrt{2\pi}}\,(1 + O(1/x^2)) \tag{81}$$

see, e.g., [1]. Using (81), we find that for large γ, i.e., high SNRs, the exponent X as introduced in (67) is

$$\begin{aligned} X_\mu &= -sb + n \ln g_\mu(s) \\ &= \begin{cases} -sb, & \text{if } s \le \gamma/(1+\mu) \\ -sb + n(s(1+\mu) - \gamma), & \text{if } s > \gamma/(1+\mu) \end{cases} \end{aligned} \tag{82}$$

in case $\mathcal{R} = \mathcal{R}_\mu$ with $\mu \in [0, 1]$, and

$$\begin{aligned} X_m &= -sb + n \ln g_m(s) \\ &= \begin{cases} -sb, & \text{if } s \le \gamma m/(m+1) \\ -sb + n\left(s\,\frac{m+1}{m} - \gamma\right), & \text{if } s > \gamma m/(m+1) \end{cases} \end{aligned} \tag{83}$$

in case $\mathcal{R} = \mathcal{R}_m$ with $m \in \{1, 3, 5, \ldots\}$, and

$$\begin{aligned} X_m &= -sb + n \ln g_m(s) \\ &= \begin{cases} -sb, & \text{if } s \le 2m\gamma\left(m + 1 - \sqrt{m^2 + 2m}\right) \\ -sb + n & \\ \cdot \left(-\gamma + s\,\frac{m+1}{m}\right. & \\ \left. \quad - \frac{s^2}{4m^2\gamma}\right), & \text{if } 2m\gamma\left(m + 1 - \sqrt{m^2 + 2m}\right) \\ & \quad < s \le 2m\gamma \\ -sb + ns, & \text{if } s > 2m\gamma \end{cases} \end{aligned} \tag{84}$$

in case $\mathcal{R} = \mathcal{R}_m$ with $m \in \{2, 4, 6, \ldots\}$. Since $b \le 2r_{\mathrm{G}}(d, \mathcal{R})$, we find from Corollary 2 that the s minimizing (82) is

$$s_\mu = \gamma/(1+\mu), \qquad \text{for } \mu \in [0, 1] \tag{85}$$

and, from Corollary 3, that the s minimizing (83) is

$$s_m = \gamma m/(m+1), \qquad \text{for } m \in \{1, 3, 5, \ldots\} \tag{86}$$

and the s minimizing (84) is

$$s_m = 2m\gamma\left(m + 1 - \sqrt{m^2 + 2m}\right), \qquad \text{for } m \in \{2, 4, 6, \ldots\} \tag{87}$$

which gives

$$X_v = -bs_v \tag{88}$$

as the minimal exponent for $v \in [0, 1] \cup \{1, 2, 3, \ldots\}$. Hence, for SNR approaching infinity, the probability of unsuccessful decoding for a reduced decoder (with reliability set $\mathcal{R}_v$ and erasing algorithm $\mathcal{A}$) is essentially $e^{-bs_v} = e^{-2r_{\mathrm{G}}(\mathcal{C}, \mathcal{R}_v, \mathcal{A})s_v}$. Since this probability is asymptotically $e^{-\gamma d}$ for ML decoding [7], Theorem 7 follows.

Acknowledgment

The authors wish to thank the anonymous reviewers and the Associate Editor for their suggestions that improved the quality of this correspondence.

References

[1] M. Abramowitz and I. A. Stegun, Eds., *Handbook of Mathematical Functions*. New York: Dover, 1965.

[2] D. Agrawal and A. Vardy, "Generalized minimum distance decoding in Euclidean space: Performance analysis," *IEEE Trans. Inform. Theory*, vol. 46, pp. 60–83, Jan. 2000.

[3] I. M. Boyarinov, "Method of decoding direct sums of products of codes and its applications," *Probl. Pered. Inform.*, vol. 17, no. 2, pp. 39–51, 1981.

[4] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 170–181, Jan. 1972.

[5] I. Dumer, "Concatenated codes and their multilevel generalizations," in *Handbook of Coding Theory*, R. Brualdi, C. Huffman, and V. Pless, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[6] G. D. Forney, Jr., "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. IT-12, pp. 125–131, Apr. 1966.
[7] ——, *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.
[8] M. P. C. Fossorier and S. Lin, "A unified method for evaluating the error-correction radius of reliability-based soft-decision algorithms for linear block codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 691–700, Mar. 1998.
[9] ——, "Chase-type and GMD coset decodings," *IEEE Trans. Commun.*, vol. 48, pp. 345–350, Mar. 2000.
[10] ——, "Error performance analysis for reliability-based decoding algorithms," *IEEE Trans. Inform. Theory*, vol. 48, pp. 287–293, Jan. 2002.
[11] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1986.
[12] S. I. Kovalev, "Two classes of minimum generalized distance decoding algorithms," *Probl. Pered. Inform.*, vol. 22, no. 3, pp. 35–42, 1986.
[13] Y. Liu, H. Tang, S. Lin, and M. Fossorier, "An interactive concatenated turbo coding system," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 367.
[14] D. J. Taipale and M. B. Pursley, "An improvement to generalized-minimum-distance decoding," *IEEE Trans. Inform. Theory*, vol. 37, pp. 167–172, Jan. 1991.
[15] H. Tanaka and K. Kakigahara, "Simplified correlation decoding by selecting possible codewords using erasure information," *IEEE Trans. Inform. Theory*, vol. IT–29, pp. 743–748, Sept. 1983.
[16] V. V. Zyablov, "Optimization of concatenated decoding algorithms," *Probl. Pered. Inform.*, vol. 9, no. 1, pp. 26–32, 1973.

Alternative Structure for Computing APPs of the Markov Source

Jongseung Park, *Member, IEEE,* and
Jaekyun Moon, *Senior Member, IEEE*

***Abstract*—We introduce an alternative structure for computing the *a posteriori* probabilities (APPs) for state and transition sequences of a Markov source observed through a noisy output sequence. Compared to the well-established forward–backward recursion algorithm of Bahl *et al.*, the proposed structure allows a reduction in computational complexity at the expense of increased memory requirements. Alternatively, for a similar complexity level, the proposed structure needs smaller memory when the input alphabet size is small.**

***Index Terms*—A posteriori probability (APP), Bahl–Cocke–Jelinek–Raviv (BCJR) algorithm, Markov source, soft decision.**

I. Introduction

Generating reliable soft decisions is essential for iterative decoders to improve their performance beyond conventional hard-decision decoding [1]–[3]. When the observation sequence is the output of a finite-state Markov source corrupted by additive white Gaussian noise (AWGN), the well-known Bahl–Cocke–Jelinek–Raviv (BCJR) algorithm provides a means to compute *a posteriori* probabilities (APPs) or optimal soft decisions for the input symbols [4]. In this correspondence, we introduce an alternative formulation of the optimal APP algorithm that leads to different computation and memory tradeoffs. The present formulation allows reduced computational complexity at the cost of an increased memory size, relative to the BCJR algorithm. Alternatively, for a comparable level of complexity, the proposed structure enables a savings in memory requirement, especially for small alphabet sizes. The proposed algorithm also works based on forward and backward recursions of the probability computations, but the recursion in one direction does not explicitly compute or retrieve the branch metrics.

Manuscript received July 24, 2001; revised November 7, 2002. This work was supported in part by the National Science Foundation under Grant CCR-9805195.

J. Park was with the Communications and Data Storage Laboratory, Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA. He is now with Seagate Technology, Pittsburgh, PA 15222 USA (e-mail: Jongseung.Park@Seagate.com).

J. Moon is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: moon@ece.umn.edu).

Communicated by A. Kavčić, Associate Editor for Detection and Estimation.
Digital Object Identifier 10.1109/TIT.2003.809500

II. Proposed Formulation for APP Computation

The noisy observation on the output of a Markov source can be expressed as

$$Y_k = L(b_k, b_{k-1}, \ldots, b_{k-I}) + n_k \tag{1}$$

where $L(\cdot)$ is an arbitrary but known function, b_k is the input taken from a finite alphabet, and n_k denotes the AWGN samples. Defining the state variable $S_k = \{b_k, b_{k-1}, \ldots, b_{k-I+1}\}$, the noise-free portion of Y_k is also fully determined by S_{k-1} and b_k. As discussed in [4], APPs of the input can be computed from the APPs of the states or state transitions, which, in turn, can be obtained by normalizing the joint state probabilities

$$\lambda_k(m) = p(S_k = m,\ \boldsymbol{Y}) \tag{2}$$

or the joint state transition probabilities

$$\sigma_k(m', m) = p(S_{k-1} = m',\ S_k = m,\ \boldsymbol{Y}) \tag{3}$$

where $\boldsymbol{Y}$ denotes the entire sequence of observation. The partial trellis shown in Fig. 1 further clarifies the notations.We can write

$$\begin{aligned}\lambda_k(m) &= \sum_{m'} p(S_{k-1} = m',\ S_k = m,\ \boldsymbol{Y}) \\ &= \sum_{m'} P(S_k = m | S_{k-1} = m',\ \boldsymbol{Y}) p(S_{k-1} = m',\ \boldsymbol{Y}) \\ &= \sum_{m'} \eta_k(m',\ m)\lambda_{k-1}(m')\end{aligned} \tag{4}$$

where

$$\begin{aligned}\eta_k(m', m) &= P(S_k = m | S_{k-1} = m',\ \boldsymbol{Y}) \\ &= P(S_k = m | S_{k-1} = m', Y_k^N)\end{aligned} \tag{5}$$

with Y_k^N denoting the collection of the observation samples Y_k through the last sample Y_N. The second equality in (4) follows since the probability of S_k does not depend on the previous observations once S_{k-1} is known. Equation (4) represents the forward recursion. Next we show how $\eta_k(m',\ m)$ is computed using a backward recursion and a subsequent normalization. First define the probability functions

$$\begin{aligned}\phi_k(m', m) &= p(S_k = m,\ Y_k^N | S_{k-1} = m') \\ &= \sum_{S_{k+1}^N} p(S_k = m,\ S_{k+1}^N,\ Y_k^N | S_{k-1} = m') \\ &= \sum_{S_{k+1}^N} p(Y_k^N | S_{k-1} = m',\ S_k = m,\ S_{k+1}^N) \\ &\quad \times P(S_k = m,\ S_{k+1}^N | S_{k-1} = m')\end{aligned} \tag{6}$$