On Multiple Decoding Attempts for Reed-Solomon Codes: A Rate-Distortion Approach

Phong S. Nguyen, *Student Member, IEEE*, Henry D. Pfister, *Member, IEEE*, and
Krishna R. Narayanan, *Senior Member, IEEE*

Abstract

One popular approach to soft-decision decoding of Reed-Solomon (RS) codes is based on using multiple trials of a simple RS decoding algorithm in combination with erasing or flipping a set of symbols or bits in each trial. This paper presents a framework based on rate-distortion (RD) theory to analyze these multiple-decoding algorithms. By defining an appropriate distortion measure between an error pattern and an erasure pattern, the successful decoding condition, for a single errors-and-erasures decoding trial, becomes equivalent to distortion being less than a fixed threshold. Finding the best set of erasure patterns also turns into a covering problem which can be solved asymptotically by rate-distortion theory. Thus, the proposed approach can be used to understand the asymptotic performance-versus-complexity trade-off of multiple errors-and-erasures decoding of RS codes.

This initial result is also extended a few directions. The rate-distortion exponent (RDE) is computed to give more precise results for moderate blocklengths. Multiple trials of algebraic soft-decision (ASD) decoding are analyzed using this framework. Analytical and numerical computations of the RD and RDE functions are also presented. Finally, simulation results show that sets of erasure patterns designed using the proposed methods outperform other algorithms with the same number of decoding trials.

This work was supported by the National Science Foundation under Grant No. 0802124. The work of P. S. Nguyen was also supported in part by a Vietnam Education Foundation fellowship. The material in this paper was presented in part at the 47th Annual Allerton Conference on Communications, Control and Computing, Monticello, IL, October 2009 and in part at IEEE International Symposium on Information Theory (ISIT), Austin, TX, June 2010.

The authors are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA (email: psn@tamu.edu; hpfister@tamu.edu; krn@tamu.edu).

I. Introduction

Reed-Solomon (RS) codes are among the most popular error-correcting codes in communication and data storage systems. An (N, K) RS code of length N and dimension K is a maximum distance separable (MDS) linear code with minimum distance $d_{\min} = N - K + 1$. RS codes have efficient hard-decision decoding (HDD) algorithms, such as the Berlekamp-Massey (BM) algorithm, which can correct up to $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ errors.

Since the discovery of RS codes [1], researchers have spent a considerable effort on improving the decoding performance at the expense of complexity. A breakthrough result of Guruswami and Sudan (GS) introduced an algebraic hard-decision list-decoding algorithm, based on bivariate interpolation and factorization, that can correct errors well beyond half the minimum distance of the code [2]. Nevertheless, HDD algorithms do not fully exploit the information provided by the channel output. Koetter and Vardy (KV) later extended the GS decoder to an algebraic soft-decision (ASD) decoding algorithm by converting the probabilities observed at the channel output into algebraic interpolation conditions in terms of a multiplicity matrix [3].

The GS and KV algorithms, however, have significant computational complexity. Therefore, multiple runs of errors-and-erasures and errors-only decoding with some low-complexity algorithm, such as the BM algorithm, has renewed the interest of researchers. These algorithms use the soft-information available at the channel output to construct a set of either erasure patterns [4], [5], test patterns [6], or patterns combining both [7], [8] and then attempt to decode using each pattern. Techniques have also been introduced to lower the complexity per decoding trial in [9], [10], [11]. Other soft-decision decoding algorithms for RS codes include [12], [13] that use the binary expansion of RS codes to work on the bit-level. In [12], belief propagation is run while the parity-check matrix is iteratively adapted on the least reliable basis. Meanwhile, [13] adapts the generator matrix on the most reliable basis and uses reprocessing techniques based on ordered statistics.

In the scope of multiple errors-and-erasures decoding, there have been several algorithms proposed that use different erasure codebooks (i.e., different sets of erasure patterns). After running the errors-and-erasures decoding algorithm multiple times, each time using one erasure pattern in the set, these algorithms produce a list of candidate codewords, whose size is usually small, and then pick the best codeword on this list. The common idea of constructing the set of erasure patterns in these multiple errors-and-erasures decoding algorithms is to erase some of the least reliable symbols since those symbols are more prone to be erroneous. The first algorithm of this type is called Generalized Minimum Distance

(GMD) [4] and it repeats errors-and-erasures decoding while successively erasing an even number of the least reliable positions (LRPs) (assuming that $d_{\min}$ is odd). More recent work by Lee and Kumar [5] proposes a soft-information successive (multiple) error-and-erasure decoding (SED) that achieves better performance but also increases the number of decoding attempts. Literally, the Lee-Kumar's SED(l, f) algorithm runs multiple errors-and-erasures decoding trials with every combination of an even number $\leq f$ of erasures within the l LRPs.

A natural question that arises is how to construct the "best" set of erasure patterns for multiple errors-and-erasures decoding. Inspired by this, we first develop a rate-distortion (RD) framework to analyze the asymptotic trade-off between performance and complexity of multiple errors-and-erasures decoding of RS codes. The main idea is to choose an appropriate distortion measure so that the decoding is successful if and only if the distortion between the error pattern and erasure pattern is smaller than a fixed threshold. After that, a set of erasure patterns is generated randomly (similar to a random codebook generation) in order to minimize the expected minimum distortion.

One of the drawbacks in the RD approach is that the mathematical framework is only valid as the block-length goes to infinity. Therefore, we also consider the natural extension to a rate-distortion exponent (RDE) approach that studies the behavior of the probability, p_e, that the transmitted codeword is not on the list as a function of the block-length N. The overall error probability can be approximated by p_e because the probability that the transmitted codeword is on the list but not chosen is very small compared to p_e. Hence, our RDE approach essentially focuses on maximizing the exponent at which the error probability decays as N goes to infinity. The RDE approach can also be considered as the generalization of the RD approach since the latter is a special case of the former when the rate-distortion exponent tends to zero. Using the RDE analysis, this approach also helps answer the following two questions: (i) What is the minimum error probability achievable for a given number of decoding attempts (or a given size of the set of erasure patterns)? (ii) What is the minimum number of decoding attempts required to achieve a certain error probability?

The RD and RDE approaches are also extended beyond conventional errors-and-erasures decoding to analyze multiple-decoding for decoding schemes such as ASD decoding. It is interesting to note that the RDE approach for ASD decoding schemes contains the special case where the codebook has exactly one entry (i.e., ASD decoding is run only once). In this case, the distribution of the codebook that maximizes the exponent implicitly generates the optimal multiplicity matrix. This is similar to the line of work [14], [15], [16], [17] where various researchers solve for a multiplicity matrix that minimizes the error probability obtained by either using a Gaussian approximation [14], applying a Chernoff bound [15],

[16], or using Sanov's theorem [17].

Finally, we propose a family of multiple-decoding algorithms based on these two approaches that achieve better performance-versus-complexity trade-off than other algorithms.

A. Outline of the paper

The paper is organized as follows. In Section II, we design an appropriate distortion measure and present a rate-distortion framework, for both the RD and RDE approaches, to analyze the performance-versus-complexity trade-off of multiple errors-and-erasures decoding of RS codes. Also in this section, we propose a general multiple-decoding algorithm that can be applied to errors-and-erasures decoding. Then, in Section III, we discuss numerical computations of RD and RDE functions together with their complexity analyses which are needed for the proposed algorithm. In Section IV, we analyze both bit-level and symbol-level ASD decoding and design distortion measures compatible with the general algorithm. A closed-form analysis of some RD and RDE functions is presented in Section V. Next, in Section VI, we offer some extensions that combine covering codes with random codes and also consider the case of a single decoding attempt. Simulation results are presented in Section VII and, finally, conclusions are provided in Section VIII.

II. A RD Framework For Multiple Errors-and-Erasures Decoding

In this section, we first set up a rate-distortion framework to analyze multiple attempts of conventional hard decision errors-and-erasures decoding.

Let $\mathbb{F}_m$ with $m = 2^\eta$ be the Galois field with m elements denoted as $\alpha_1, \alpha_2, \ldots, \alpha_m$. We consider an (N, K) RS code of length N, dimension K over $\mathbb{F}_m$. Assume that we transmit a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_N) \in \mathbb{F}_m^N$ over some channel and receive a vector $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathcal{Y}^N$ where $\mathcal{Y}$ is the received alphabet for a single RS symbol. While our approach can be applied to much more general channels, our simulations focus on the Additive White Gaussian Noise (AWGN) channel and two common modulation formats, namely BPSK and m-QAM. Correspondingly, we use $\mathcal{Y} = \mathbb{R}^\eta$ for BPSK and $\mathcal{Y} = \mathbb{R}^2$ for m-QAM. For each codeword index i, let $\varphi_i : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$ be the permutation given by sorting $\pi_{i,j} = \Pr(c_i = \alpha_j | r_i)$ in decreasing order so that $\pi_{i,\varphi_i(1)} \geq \pi_{i,\varphi_i(2)} \geq \ldots \geq \pi_{i,\varphi_i(m)}$. Then, we can specify $y_{i,j} = \alpha_{\varphi_i(j)}$ as the j-th most reliable symbol for $j = 1, \ldots, m$ at codeword index i. To obtain the reliability of the codeword positions (indices), we construct the permutation $\sigma : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$ given by sorting the probabilities $\pi_{i,\varphi_i(1)}$ of the most likely symbols in increasing order.[1] Thus, codeword position $\sigma(i)$ is the i-th LRP. These above notations will be used throughout this paper.

Example 1: Consider $N = 3$ and $m = 4$. Assume that we have the probability $\pi_{i,j}$ written in a matrix form as follows:

$$\mathbf{\Pi} = \begin{pmatrix} 0.01 & 0.01 & \mathbf{0.93} \\ \mathbf{0.94} & 0.03 & 0.04 \\ 0.03 & \mathbf{0.49} & 0.01 \\ 0.02 & 0.47 & 0.02 \end{pmatrix} \text{where } \pi_{i,j} = [\mathbf{\Pi}]_{j,i}.$$

then $\varphi_1(1,2,3,4) = (2,3,4,1)$, $\varphi_2(1,2,3,4) = (3,4,2,1)$, $\varphi_3(1,2,3,4) = (1,2,4,3)$ and $\sigma(1,2,3) = (2,3,1)$.

Condition 1: (Classical decoding threshold, see [18], [19]): If e symbols are erased, a conventional hard-decision errors-and-erasures decoder such as the BM algorithm is able to correct ν errors in unerased positions if and only if

$$2\nu + e < N - K + 1. \tag{1}$$

A. Conventional error patterns and erasure patterns.

Definition 1: (Conventional error patterns and erasure patterns) We define $x^N \in \mathbb{Z}_2^N \triangleq \{0,1\}^N$ and $\hat{x}^N \in \mathbb{Z}_2^N$ as an error pattern and an erasure pattern respectively, where $x_i = 0$ means that an error occurs (i.e., the most likely symbol is incorrect) and $\hat{x}_i = 0$ means that the symbol at index i is erased (i.e., an erasure is applied at index i). X^N and $\hat{X}^N$ will be used to denote the random vectors which generate the realizations x^N and $\hat{x}^N$, respectively.

Example 2: If $d_{\min}$ is odd then the GMD algorithm corresponds to the set

$$\{111111\ldots, 001111\ldots, 000011\ldots, \ldots, \underbrace{00\ldots0}_{d_{\min}-1}11\ldots1\}$$

of erasure patterns. Meanwhile, the SED$(3,2)$ uses the following set

$$\{\underline{111}111\ldots, \underline{001}111\ldots, \underline{010}111\ldots, \underline{100}111\ldots\}.$$

Here, in each erasure pattern, the letters are written in increasing reliability order of the codeword positions.

Let us revisit the question of how to construct the best set of erasure patterns for multiple errors-and-erasures decoding. First, it can be seen that a multiple errors-and-erasures decoding succeeds if the

[1] Other measures such as entropy or the average number of guesses might improve Algorithm B in Section II-C.

condition (1) is satisfied during at least one round of decoding. Thus, our approach is to design a distortion measure that converts the condition (1) into a form where the distortion between an error pattern x^N and an erasure pattern $\hat{x}^N$, denoted as $d(x^N, \hat{x}^N)$, is less than a fixed threshold.

Definition 2: Given a *letter-by-letter* distortion measure δ, the distortion between an error pattern x^N and an erasure pattern $\hat{x}^N$ is defined by

$$d(x^N, \hat{x}^N) = \sum_{i=1}^{N} \delta(x_i, \hat{x}_i).$$

Proposition 1: If we choose the *letter-by-letter* distortion measure $\delta : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}_{\geq 0}$, where in this case $\mathcal{X} = \hat{\mathcal{X}} = \mathbb{Z}_2$, as follows:

$$\begin{aligned} \delta(0,0) = 1, \quad \delta(0,1) = 2, \\ \delta(1,0) = 1, \quad \delta(1,1) = 0, \end{aligned} \tag{2}$$

then the condition (1) for a successful errors-and-erasures decoding is equivalent to

$$d(x^N, \hat{x}^N) < N - K + 1 \tag{3}$$

where the distortion is less than a fixed threshold.

Proof: First, we define

$$\chi_{j,k} \triangleq |\{i \in \{1, 2, \ldots, N\} : x_i = j, \hat{x}_i = k\}|$$

to count the number of $(x_i, \hat{x}_i)$ pairs equal to (j, k) for every $j \in \mathcal{X}$ and $k \in \hat{\mathcal{X}}$. With the chosen distortion measure, we have

$$d(x^N, \hat{x}^N) = 2\chi_{0,1} + \chi_{0,0} + \chi_{1,0}.$$

Noticing that $e = \chi_{0,0} + \chi_{1,0}$ and $\nu = \chi_{0,1}$, the condition (1) for one errors-and-erasures decoding attempt to succeed becomes $2\chi_{0,1} + \chi_{0,0} + \chi_{1,0} < N - K + 1$ which is equivalent to $d(x^N, \hat{x}^N) < N - K + 1$.

■

Next, we try to maximize the chance that this successful decoding condition is satisfied by at least one of the decoding attempts (i.e., $d(x^N, \hat{x}^N) < N - K + 1$ for at least one erasure pattern $\hat{x}^N$). Mathematically, we want to build a set $\mathcal{B}$ of no more than 2^R erasure patterns $\hat{x}^N$ that achieves the maximum

$$\max_{\mathcal{B}:|\mathcal{B}| \leq 2^R} \Pr\left\{ \min_{\hat{x}^N \in \mathcal{B}} d(X^N, \hat{x}^N) < N - K + 1 \right\}.$$

Solving this problem exactly is very difficult. However, one can observe that it is a covering problem where tries to cover the most-likely error patterns using a fixed number of spheres centered at the chosen erasure patterns. This view leads to two asymptotic solutions of the problem based on rate-distortion theory. Taking this point of view, we view the error pattern x^N as a source sequence and the erasure pattern $\hat{x}^N$ as a reproduction sequence.

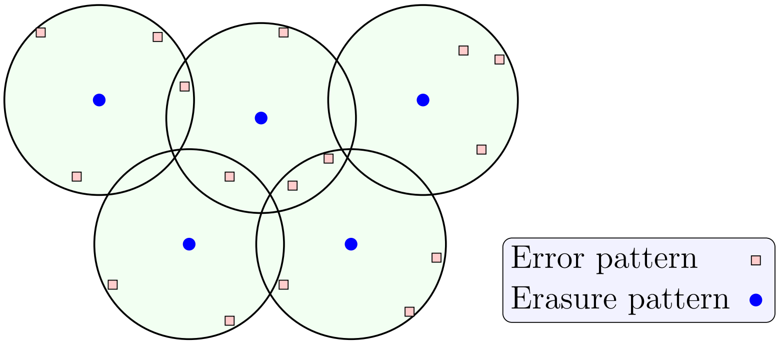

Fig. 1. Pictorial illustration of a covering problem

1) RD approach: Rate-distortion theory (see [20, Chapter 13]) characterizes the trade-off between $\bar{R}$ and $\bar{D}$ such that sets $\mathcal{B}$ of $2^{N\bar{R}}$ reproduction sequences exist (and can be generated randomly) so that

$$\lim_{N\to\infty} \frac{1}{N} E_{X^N,\mathcal{B}} \left[\min_{\hat{x}^N\in\mathcal{B}} d(X^N,\hat{x}^N) \right] < \bar{D}.$$

Under mild conditions, this implies that, for large enough N, we have

$$\min_{\hat{x}^N\in\mathcal{B}} d(X^N,\hat{x}^N) < N\bar{D}$$

with high probability. Here, $\bar{R}$ and $\bar{D}$ are closely related to the complexity and the performance, respectively, of the decoding algorithm. Therefore, we characterize the trade-off between those two aspects using the relationship between $\bar{R}$ and $\bar{D}$. In this paper, we denote the rate and distortion by R and D, respectively, using unnormalized quantities, i.e., $R = N\bar{R}$ and $D = N\bar{D}$.

2) RDE approach: The above-mentioned RD approach focuses on minimizing the average minimum distortion with little knowledge of how the tail of the distribution behaves. In this RDE approach, we instead focus on directly minimizing the probability that the minimum distortion is not less than the predetermined threshold $D = N - K + 1$ (due to the condition (3)) with the help of an error-exponent analysis. The exact probability of interest is

$$p_e = \Pr\left(X^N : \min_{\hat{x}^N\in\mathcal{B}} d(X^N,\hat{x}^N) > D \right)$$

that reflects how likely the decoding threshold (1) is going to fail. In other words, every error pattern x^N can be covered by a sphere centered at an erasure pattern $\hat{x}^N$ except for a set of error patterns of probability p_e. The RDE analysis shows that p_e decays exponentially as $N \to \infty$ and the maximum exponent attainable is the RDE function $F(R,D)$. Throughout this paper, we denote the rate-distortion exponent by $F(R,D)$ using unnormalized quantities (i.e., without dividing by N) and note that exponent used by other authors in [21], [22], [23] is often the normalized version $\bar{F}(R,D) \triangleq \frac{F(R,D)}{N}$.

RDE analysis is discussed extensively in [21], [22] and it is shown that a set $\mathcal{B}$ of roughly $2^{N\bar{R}}$ codewords, generated randomly using the test-channel input distribution, can be used to achieve $\bar{F}(R,D)$. An upper bound is also given that shows, for any $\epsilon > 0$, there is a sufficiently large N (see [24, p. 229]) such that

$$p_e \leq 2^{-N[\bar{F}(R,D)-\epsilon]}.$$

An exponentially tight lower bound for p_e can also be obtained (see [24, p. 236]) and it implies that the best sequence of codebooks satisfy

$$\lim_{N\to\infty} -\frac{1}{N}\log p_e = \bar{F}(R,D).$$

Remark 1: The RDE approach possesses several advantages. First, the converse of the RDE [24, p. 236] provides a lower bound for p_e. This implies that, given an arbitrary set $\mathcal{B}$ of roughly $2^{N\bar{R}}$ erasure patterns and any $\epsilon > 0$, the probability p_e cannot be made lower than $2^{-N[\bar{F}(R,D)+\epsilon]}$ for N large enough. Thus, no matter how one chooses the set $\mathcal{B}$ of erasure patterns, the difference between the induced probability of error and the p_e for the RDE approach becomes negligible for N large enough. Second, it can help one estimate the smallest number of decoding attempts to get to a RDE of F (or get to an error probability of roughly $2^{-N\bar{F}}$) or, similarly, allow one to estimate the RDE (and error probability) for a fixed number of decoding attempts.

B. Generalized error patterns and erasure patterns

In this subsection, we consider a generalization of the conventional error patterns and erasure patterns under the same framework to make better use of the soft information. At each index of the RS codeword, besides erasing a symbol, we also try to decode using not only the most likely symbol but also less likely ones as the hard decision (HD) symbol. To handle up to the ℓ most likely symbols at each index i, we let $\mathbb{Z}_{\ell+1} \triangleq \{0,1,\ldots,\ell\}$ and consider the following definition.

Definition 3: (Generalized error patterns and erasure patterns) Consider a positive integer ℓ smaller than the field size m. Let $x^N \in \mathbb{Z}_{\ell+1}^N$ be a *generalized error pattern* where, at index i, $x_i = j$ implies that the j-th most likely symbol is correct for $j \in \{1,2,\ldots\ell\}$, and $x_i = 0$ implies none of the first ℓ most likely symbols is correct. Let $\hat{x}^N \in \mathbb{Z}_{\ell+1}^N$ be a *generalized erasure pattern* used for decoding where, at index i, $\hat{x}_i = k$ implies that the k-th most likely symbol is used as the hard-decision symbol for $k \in \{1,2,\ldots,\ell\}$, and $\hat{x}_i = 0$ implies that an erasure is used at that index.

For simplicity, we refer to x^N as the error pattern and $\hat{x}^N$ as the erasure pattern like in the conventional case. Now, we need to convert the condition (1) to the form where $d(x^N, \hat{x}^N)$ is less than a fixed threshold. Proposition 1 is thereby generalized into the following proposition.

Proposition 2: We choose the *letter-by-letter* distortion measure $\delta : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}_{\geq 0}$, where in this case $\mathcal{X} = \hat{\mathcal{X}} = \mathbb{Z}_{\ell+1}$, defined by $\delta(x, \hat{x}) = [\Delta]_{x,\hat{x}}$ in terms of the $(\ell + 1) \times (\ell + 1)$ matrix

$$\Delta = \begin{pmatrix} 1 & 2 & \ldots & 2 & 2 \\ 1 & 0 & \ldots & 2 & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 2 & \ldots & 0 & 2 \\ 1 & 2 & \ldots & 2 & 0 \end{pmatrix}. \tag{4}$$

Using this, the condition (1) for a successful errors-and-erasures decoding is equivalent to

$$d(x^N, \hat{x}^N) < N - K + 1.$$

Proof: The reasoning is very similar to the proof of Proposition 1 using the fact that $e = \sum_{j=0}^{\ell} \chi_{j,0}$ and $\nu = \sum_{k=1}^{\ell} \sum_{j=0, j\neq k}^{\ell} \chi_{j,k}$ where $\chi_{j,k} \triangleq |\{i \in \{1, 2, \ldots, N\} : x_i = j, \hat{x}_i = k\}|$ for every $j, k \in \mathbb{Z}_{\ell+1}$. ■

For each $\ell = 1, 2, \ldots, m$, we will refer to this generalized case as mBM-ℓ decoding.

Example 3: Consider mBM-2 (or top-ℓ decoding with $\ell = 2$). In this case, the distortion measure is given by following the matrix

$$\Delta = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}.$$

Remark 2: The distortion measure matrix changes slightly if we use the errors-only decoding instead of errors-and-erasures decoding. In this case, $\hat{\mathcal{X}} = \mathbb{Z}_{\ell+1} \setminus \{0\}$ and the chosen letter-by-letter distortion measure is given in terms of the $(\ell + 1) \times \ell$ matrix obtained by deleting the first column of (4). When $\ell = 2$, we consider the first and second most likely symbols as the two hard-decision symbols at each codeword position. This is similar to the Chase-type decoding method proposed by Bellorado and Kavcic [9]. Das and Vardy also suggest this approach by considering only several highest entries in each column of the reliability matrix Π for single ASD decoding of RS codes [17].

C. Proposed General Multiple-Decoding Algorithm

In this section, we propose two general multiple-decoding algorithms for RS codes. In each algorithm, one can choose either Step 2a that corresponds to the RD approach or Step 2b that corresponds to the

RDE approach. These general algorithms apply to not only multiple errors-and-erasures decoding but also multiple-decoding of other decoding schemes that we will discuss later. The common first step is designing a distortion measure $\delta : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}_{\geq 0}$ that converts the condition for a single decoding to succeed to the form where distortion is less than a fixed threshold. After that, decoding proceeds as described below.

1) Algorithm A:

Step 1: Based on the received signal sequence, compute an $m \times N$ reliability matrix $\mathbf{\Pi}$ where $[\mathbf{\Pi}]_{j,i} = \pi_{i,j}$. From this, determine the probability matrix $\mathbf{P}$ where $p_{i,j} = \Pr(X_i = j)$ for $i = 1, 2, \ldots, N$ and $j \in \mathcal{X}$.

Step 2a: (RD approach) Compute the RD function of a source sequence (error pattern) with probability of source letters derived from $\mathbf{P}$ and the chosen distortion measure (see Section III and Section V). Given the design rate R, determine the optimal input-probability distribution matrix $\mathbf{Q}$, for the test channel, with entries $q_{i,k} = \Pr(\hat{X}_i = k)$ for $i = 1, 2, \ldots, N$ and $k \in \hat{\mathcal{X}}$.

Step 2b: (RDE approach) Given D (in most cases $D = N - K + 1$) and the design rate R, compute the RDE function of a source sequence (error pattern) with probability of source letters derived from $\mathbf{P}$ and the chosen distortion measure (see Section III and Section V). Also determine the optimal input-probability distribution matrix $\mathbf{Q}$, for the test channel, with entries $q_{i,k} = \Pr(\hat{X}_i = k)$ for $i = 1, 2, \ldots, N$ and $k \in \hat{\mathcal{X}}$.

Step 3: Randomly generate a set of 2^R erasure patterns using the test-channel input-probability distribution matrix $\mathbf{Q}$.

Step 4: Run multiple attempts of the corresponding decoding scheme (e.g., errors-and erasures decoding) using the set of erasure patterns in Step 3 to produce a list of candidate codewords.

Step 5: Use the maximum-likelihood (ML) rule to pick the best codeword on the list.

Remark 3: In Algorithm A, the RD (or RDE) function is computed on the fly, i.e., after every received signal sequence. In practice, it may be preferable to precompute the RD (or RDE) function based on the empirical distribution measured from the channel. We refer to this approach as Algorithm B, and simulation results show a negligible difference in the performance of these two algorithms.

2) Algorithm B:

Step 1: Transmit τ (e.g., $\tau = 10^3 - 10^6$) arbitrary test RS codewords, indexed by time $t = 1, 2, \ldots, \tau$, over the channel and compute a set of τ $m \times N$ matrices $\mathbf{\Pi}_1^{(t)}$ where $[\mathbf{\Pi}_1^{(t)}]_{j,i} = \pi^{(t)}_{i,\varphi_i^{(t)}(j)}$ is the probability of the j-th most likely symbol at position i during time t. For each time t, obtain the matrix $\mathbf{\Pi}_2^{(t)}$ from $\mathbf{\Pi}_1^{(t)}$ through a permutation $\sigma^{(t)} : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$ that sorts the probabilities $\pi^{(t)}_{i,\varphi_i^{(t)}(1)}$ in increasing order to indicate the reliability order of codeword positions. Take the entry-wise average of all τ matrices $\mathbf{\Pi}_2^{(t)}$ to get an average matrix $\bar{\mathbf{\Pi}}$.[2] The matrix $\bar{\mathbf{\Pi}}$ serves as $\mathbf{\Pi}$ in Algorithm A and from this, determine the probability matrix $\mathbf{P}$ where $p_{i,j} = \Pr(X_i = j)$ for $i = 1, 2, \ldots, N$ and $j \in \mathcal{X}$.

Step 2a: (RD approach) Compute the RD function of a source sequence (error pattern) with probability of source letters derived from $\mathbf{P}$ and the chosen distortion measure. Given a design rate R, determine the test-channel input-probability distribution matrix $\mathbf{Q}$ where $q_{i,k} = \Pr(\hat{X}_i = k)$ for $i = 1, 2, \ldots, N$ and $k \in \hat{\mathcal{X}}$.

Step 2b: (RDE approach) Given D (in most cases $D = N - K + 1$) and the design rate R, compute the RDE function of a source sequence (error pattern) with probability of source letters derived from $\mathbf{P}$ and the chosen distortion measure. Also determine the optimal test-channel input-probability distribution matrix $\mathbf{Q}$ where $q_{i,k} = \Pr(\hat{X}_i = k)$ for $i = 1, 2, \ldots, N$ and $k \in \hat{\mathcal{X}}$.

Step 3: Based on the actual received signal sequence, compute $\pi_{i,\varphi_i(1)}$ and determine the permutation σ that gives the reliability order of codeword positions by sorting $\pi_{i,\varphi_i(1)}$ in increasing order.

Step 4: Randomly generate a set of 2^R erasure patterns using the test-channel input-probability distribution matrix $\mathbf{Q}$ and permute the indices of each erasure pattern by the permutation σ^{-1}.

Step 5: Run multiple attempts of the corresponding decoding scheme (e.g., errors-and-erasures decoding) using the set of erasure patterns in Step 4 to produce a list of candidate codewords.

Step 6: Use the ML rule to pick the best codeword on the list.

III. Computing The RD and RDE Functions

In this section, we will discuss some numerical methods to compute the RD and RDE functions and the corresponding test-channel input-probability distribution matrix $\mathbf{Q}$, whose entries are $q_{i,k} = \Pr(\hat{X}_i = k)$ for $i = 1, 2, \ldots, N$ and $k \in \hat{\mathcal{X}}$. These numerical methods allow us to efficiently compute the RD and RDE functions discussed in the previous section for arbitrary discrete distortion measures. For some simple distortion measures, closed-form solutions are given in Section V.

A. Computing the RD function

For an arbitrary discrete distortion measure, it can be difficult to compute the RD function analytically. Fortunately, for a single source X, the Blahut algorithm (see details in [25]) gives an alternating

[2] In fact, one need not store separately each $\Pi_2^{(t)}$ matrix. The average $\bar{\Pi}$ can be computed on the fly.

minimization technique that efficiently computes the RD function which is given by[3]

$$R(D) = \min_{\mathbf{w} \in \mathcal{W}_D} \sum_j \sum_k p_j w_{k|j} \log \frac{w_{k|j}}{\sum_{j'} p_{j'} w_{k|j'}}$$

where $p_j \triangleq \Pr(X = j)$, $q_k \triangleq \Pr(\hat{X} = k)$, $w_{k|j} \triangleq \Pr(\hat{X} = k|X = j)$, and[4]

$$\mathcal{W}_D = \left\{ \mathbf{w} \middle| \begin{array}{c} w_{k|j} \geq 0, \sum_k w_{k|j} = 1 \\ \sum_j \sum_k p_j w_{k|j} \delta_{jk} \leq D \end{array} \right\}.$$

More precisely, given the Lagrange multiplier $t \leq 0$ that represents the slope of the RD curve at a specific point (see [26, Thm 2.5.1]) and an arbitrary all-positive initial test-channel input-probability distribution vector $\mathrm{q}^{(0)}$, the Blahut algorithm shows us how to compute the rate-distortion pair (R_t, D_t).

However, it is not straightforward to apply the Blahut algorithm to compute the RD for a discrete source sequence x^N (an error pattern in our context) of N independent but not necessarily identical (i.n.d.) source components x_i. In order to do that, we consider the group of source letters $(j_1, j_2, \ldots, j_N)$ where $j_i \in \mathcal{X}$ as a super-source letter $\mathcal{J} \in \mathcal{X}^N$, the group of reproduction letters $(k_1, k_2, \ldots, k_N)$ where $k_i \in \hat{\mathcal{X}}$ as a super-reproduction letter $\mathcal{K} \in \hat{\mathcal{X}}^N$, and the source sequence x^N as a single source. For each super-source letter $\mathcal{J}$, $p_{\mathcal{J}} = \Pr(X^N = \mathcal{J}) = \prod_{i=1}^N \Pr(X_i = j_i) = \prod_{i=1}^N p_{j_i}$ follows from the independence of source components.[5]

While we could apply the Blahut algorithm to this source directly, the complexity is a problem because the alphabet sizes for $\mathcal{J}$ and $\mathcal{K}$ become the super-alphabet sizes $|\chi|^N$ and $|\hat{\chi}|^N$ respectively. Instead, we avoid this computational challenge by choosing the initial test-channel input-probability distribution so that it can be factored into a product of N initial test-channel input-probability components, i.e., $q_{\mathcal{K}}^{(0)} = \prod_{i=1} q_{k_i}^{(0)}$. One can verify that this factorization rule still applies after every step τ of the iterative process, i.e., $q_{\mathcal{K}}^{(\tau)} = \prod_{i=1} q_{k_i}^{(\tau)}$. Therefore, the convergence of the Blahut algorithm [27] implies that the optimal distribution is a product distribution, i.e., $q_{\mathcal{K}}^{\star} = \prod_{i=1} q_{k_i}^{\star}$.

One can also finds that, for each parameter t, one only needs to compute the rate-distortion pair for each source component x_i separately and sum them together. This is captured into the following algorithm.

Algorithm 1: (Factored Blahut algorithm for RD function) Consider a discrete source sequence x^N of N i.n.d. source components x_i's with probability $p_{j_i} \triangleq \Pr(X_i = j_i)$. Given a parameter $t \leq 0$, the rate

[3] All logarithms in this paper are taken to base 2.

[4] $\delta(j, k)$ is sometimes written as δ_{jk} for convenience.

[5] In this paper, the notations p_{j_i} and $p_{i,j}$ are interchangeable. The notations q_{k_i} and $q_{i,k}$ are also interchangeable.

and the distortion for this source sequence under a specified distortion measure are given by

$$R_t = \sum_{i=1}^{N} R_{i,t} \text{ and } D_t = \sum_{i=1}^{N} D_{i,t} \tag{5}$$

where the components $R_{i,t}$ and $D_{i,t}$ are computed by the Blahut algorithm with the Lagrange multiplier t. This rate-distortion pair can be achieved by the corresponding test-channel input-probability distribution $q_{\mathcal{K}} \triangleq \Pr(\hat{X}^N = \mathcal{K}) = \prod_{i=1}^{n} q_{k_i}$ where the component probability distribution $q_{k_i} \triangleq \Pr(\hat{X}_i = k_i)$.

Remark 4: Equation (5) can also be derived from [26, Corollary 2.8.3] in a way that does not use the convergence property of the Blahut algorithm.

B. Computing the RDE function

The original RDE function $F(R, D)$, defined in [21, Sec. VI] for a single source X, is given by

$$F(R, D) = \max_{\mathbf{w}} \min_{\tilde{\mathbf{p}} \in \mathcal{P}_{R,D}} \sum_j \tilde{p}_j \log \frac{\tilde{p}_j}{p_j} \tag{6}$$

where $p_j = \Pr(X = j)$, $q_k = \Pr(\hat{X} = k)$, $w_{k|j} = \Pr(\hat{X} = k | X = j)$, and

$$\mathcal{P}_{R,D} = \left\{ \tilde{\mathbf{p}} \middle| \begin{array}{c} \sum_j \sum_k \tilde{p}_j w_{k|j} \log \frac{w_{k|j}}{\sum_{j'} \tilde{p}_{j'} w_{k|j'}} \geq R \\ \sum_j \sum_k \tilde{p}_j w_{k|j} \delta_{jk} \geq D \end{array} \right\}. \tag{7}$$

For a single source X, given two parameters $s \geq 0$ and $t \leq 0$ which are the Lagrange multipliers introduced in the optimization problem (see [21, p. 415]), the Arimoto algorithm given in [28, Sec. V] can be used to compute the exponent, rate, and distortion numerically.

In the context we consider, the source (error pattern) x^N comprises i.n.d. source components x_i's. We follow the same method as in the RD function case, i.e., by choosing the initial distribution still arbitrarily but following a factorization rule $q_{\mathcal{K}}^{(0)} = \prod_{i=1}^{N} q_{k_i}^{(0)}$, and this gives the following algorithm.

Algorithm 2: (Factored Arimoto algorithm for RDE function) Consider a discrete source x^N of i.n.d. source components x_i's with probability $p_{j_i} \triangleq \Pr(X_i = j_i)$. Given Lagrange multipliers $s \geq 0$ and $t \leq 0$, the exponent, rate and distortion under a specified distortion measure are given by

$$F|_{s,t} = \sum_{i=1}^{N} F_i|_{s,t}\,,\;\; R|_{s,t} = \sum_{i=1}^{N} R_i|_{s,t}\,,\;\; D|_{s,t} = \sum_{i=1}^{N} D_i|_{s,t}$$

where the components $F_i|_{s,t}$, $R_i|_{s,t}$, $D_i|_{s,t}$ are computed parametrically by the Arimoto algorithm.

Remark 5: Though it is standard practice to compute error-exponents using the implicit form given above, this approach may provide points that, while achievable, are strictly below the true RDE curve. The problem is that the true RDE curve may have a slope discontinuity that forces the implicit representation to have extra points. An example of this behavior for the channel coding error exponent is given by Gallager [29, p. 147]. For the i.n.d. source considered above, a cautious person could solve the problem as described and then check that the component RDE functions are differentiable at the optimum point. In this work, we largely neglect this subtlety.

C. Complexity of computing RD/RDE functions

1) Complexity of computing RD function.: For each parameter $t < 0$, if we directly apply of the original Blahut algorithm to compute the (R_t, D_t) pair, the complexity is $O(\tau_{\max}|\mathcal{X}|^N|\hat{\mathcal{X}}|^N)$ where $\tau_{\max}$ is the number of iterations in the Blahut algorithm. However, using the factored Blahut algorithm (Algorithm 1) greatly reduces this complexity to $O(\tau_{\max}|\mathcal{X}||\hat{\mathcal{X}}|N)$. In Section II-C, one of the proposed algorithms needs to compute the RD function for a design rate R. To do this, we apply the bisection method on t to find the correct t that corresponds to the chosen rate R.

- *Step 0*: Set $t_{\min} < 0$ (e.g., $t_{\min} = -10$)
- *Step 1*: If $R_{t_{\min}} > R$, go to Step 3. Else go to Step 2.
- *Step 2*: If $R_{t_{\min}} = R$ then stop. Else if $R_{t_{\min}} < R$, set $t_{\min} \leftarrow 2t_{\min}$ and go to Step 1.
- *Step 3*: Find t using the bisection method to get the correct rate R within ϵ_R.

The overall complexity of computing the RD function for a design rate R is

$$O\left(\tau_{\max}\log_2\left(\frac{-t_{\min}}{\epsilon_R}\right)|\mathcal{X}||\hat{\mathcal{X}}|N\right).$$

Now, we consider the dependence of $\tau_{\max}$ on ϵ_R. It follows from [27] that the error due to early termination of the Blahut algorithm is $O\left(\frac{1}{\tau_{\max}}\right)$. This implies that choosing $\tau_{\max} = O\left(\frac{1}{\epsilon_R}\right)$ is sufficient. However, recent work has shown that a slight modification of the Blahut algorithm can drastically increase the convergence rate [30]. For this reason, we leave the number of iterations as the separate constant $\tau_{\max}$ and do not consider its relationship to the error tolerance.

2) Complexity of computing RDE function.: Similarly, for each pair of parameters $t < 0$ and $s \geq 0$, the complexity if we directly apply of the original Arimoto algorithm to compute the $(R|_{s,t}, D|_{s,t})$ pair is $O(\tau_{\max}|\mathcal{X}|^N|\hat{\mathcal{X}}|^N)$ where $\tau_{\max}$ is the number of iterations. Instead, if the factored Arimoto algorithm (Algorithm 2) is employed, this complexity can also be reduced to $O(\tau_{\max}|\mathcal{X}||\hat{\mathcal{X}}|N)$. In one of our proposed general algorithms in Section II-C, we need to compute the RDE function for a pre-determined (R, D) pair. We use a nested bisection technique to find the Lagrange multipliers s, t that give the correct R and D.

- *Step 0*: Set $t_{\min} < 0$ and $s_{\max} > 0$ (e.g., $t_{\min} = -10$ and $s_{\max} = 2$)

- *Step 1*: If $R|_{s_{\max},t_{\min}} \leq R$, set $t_{\min} \leftarrow 2t_{\min}$ and repeat Step 1. Else go to Step 2.
- *Step 2*: Find t using the bisection method to obtain $R|_{s_{\max},t} = R$ within ϵ_R. If $D|_{s_{\max},t} > D$, go to Step 3. If $D|_{s_{\max},t} = D$ then stop. Else if $D|_{s_{\max},t} < D$, set $s_{\max} \leftarrow 2s_{\max}$ and go to Step 1.
- *Step 3*: Find s using the bisection method to get the correct distortion D within ϵ_D while with each s doing the following steps
  - *Step 3a*: If $R|_{s,t_{\min}} > R$, go to Step 3c.
  - *Step 3b*: If $R|_{s,t_{\min}} = R$, then stop. Else if $R|_{s,t_{\min}} < R$, set $t_{\min} \leftarrow 2t_{\min}$ and go to Step 1.
  - *Step 3c*: Find t using the bisection method to get the correct R within ϵ_R.

The overall complexity of computing the RD function for a design rate R is therefore

$$O\left(\tau_{\max} \log_2\left(\frac{-t_{\min}}{\epsilon_R}\right) \log_2\left(\frac{s_{\max}}{\epsilon_D}\right) |\mathcal{X}||\hat{\mathcal{X}}|N\right).$$

IV. Multiple Algebraic Soft-Decision (ASD) Decoding

In this section, we analyze and design a distortion measure to convert the condition for successful ASD decoding to a suitable form so that we can apply the general multiple-decoding algorithm to ASD decoding.

First, let us give a brief review on ASD decoding of RS codes. Let $\{\beta_1, \beta_2, \ldots, \beta_N\}$ be a set of N distinct elements in $\mathbb{F}_m$. From each message polynomial $f(X) = f_0 + f_1 X + \ldots + f_{K-1} X^{K-1}$ whose coefficients are in $\mathbb{F}_m$, we can obtain a codeword $c = (c_1, c_2, \ldots, c_N)$ by evaluating the message polynomial at $\{\beta_i\}_{i=1}^N$, i.e., $c_i = f(\beta_i)$ for $i = 1, 2, \ldots, N$. Given a received vector $\mathbf{r} = (r_1, r_2, \ldots, r_N)$, we can compute the *a posteriori* probability (APP) matrix $\mathbf{\Pi}$ as follows:

$$[\mathbf{\Pi}]_{j,i} = \pi_{i,j} = \Pr(c_i = \alpha_j | r_i) \text{ for } 1 \leq i \leq N, 1 \leq j \leq m.$$

The ASD decoding as in [3] has the following main steps.

1) *Multiplicity Assignment*: Use a particular multiplicity assignment scheme (MAS) to derive an $m \times N$ multiplicity matrix, denoted as $\mathbf{M}$, of non-negative integer entries $\{M_{i,j}\}$ from the APP matrix $\mathbf{\Pi}$.
2) *Interpolation*: Construct a bivariate polynomial $Q(X, Y)$ of minimum $(1, K-1)$ weighted degree that passes through each of the point (β_j, α_i) with multiplicity $M_{i,j}$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, N$.
3) *Factorization*: Find all polynomials $f(X)$ of degree less than K such that $Y - f(X)$ is a factor of $Q(X, Y)$ and re-evaluate these polynomials to form a list of candidate codewords.

In this paper, we denote $\mu = \max_{i,j} M_{i,j}$ as the maximum multiplicity. Intuitively, higher multiplicity should be put on more likely symbols. A higher μ generally allows ASD decoding to achieve a better performance. However, one of the drawbacks of ASD decoding is that its decoding complexity is roughly $O(N^2\mu^4)$ [31]. Even though there have been several reduced complexity variations and fast architectures as discussed in [32], [33], [34], the decoding complexity still increases rapidly with μ. Thus, in this section we will mainly work with small μ to keep the complexity affordable.

One of the main contributions of [3] is to offer a condition for successful ASD decoding represented in terms of two quantities specified as the score and the cost as follows.

Definition 4: The score $S_{\mathbf{M}}(\mathbf{c})$ with respect to a codeword $\mathbf{c}$ and a multiplicity matrix $\mathbf{M}$ is defined as

$$S_{\mathbf{M}}(\mathbf{c}) = \sum_{j=1}^{N} M_{[c_j],j}$$

where $[c_j] = i$ such that $\alpha_i = c_j$. The cost $C_{\mathbf{M}}$ of a multiplicity matrix $\mathbf{M}$ is defined as

$$C_{\mathbf{M}} = \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{N} M_{i,j}(M_{i,j}+1).$$

Condition 2: (ASD decoding threshold, see [3], [35], [31]). The transmitted codeword will be on the list if

$$(a+1)\left[S_{\mathbf{M}} - \frac{a}{2}(K-1)\right] > C_{\mathbf{M}} \tag{8}$$

for some $a \in \mathbb{N}$ such that

$$a(K-1) < S_{\mathbf{M}} \leq (a+1)(K-1). \tag{9}$$

To match the general framework, the ASD decoding threshold (or condition for successful ASD decoding) should be converted to the form where the distortion is smaller than a fixed threshold.

A. Bit-level ASD case

In this subsection, we consider multiple trials of ASD decoding using bit-level erasure patterns. A bit-level error pattern $b^n \in \mathbb{Z}_2^n$ and a bit-level erasure pattern $\hat{b}^n \in \mathbb{Z}_2^n$ have length $n = N \times \eta$ since each symbol has η bits. Similar to Definition 1 of a conventional error pattern and a conventional erasure pattern, $b_i = 0$ in a bit-level error pattern implies a bit-level error occurs and $\hat{b}_i$ in a bit-level erasure pattern implies that a bit-level erasure is applied. We also use B^N and $\hat{B}^N$ to denote the random vectors which generate the realizations b^N and $\hat{b}^N$, respectively.

From each bit-level erasure pattern, we can specify entries of the multiplicity matrix $\mathbf{M}$ using the bit-level MAS proposed in [35] as follows: for each codeword position, assign multiplicity 2 to the symbol with no bit erased, assign multiplicity 1 to each of the two candidate symbols if there is 1 bit erased, and assign multiplicity zero to all the symbols if there are ≥ 2 bits erased. All the other entries are zeros by default. This MAS has a larger decoding region compared to the conventional errors-and-erasures decoding scheme.

Condition 3: (Bit-level ASD decoding threshold, see [35]) For RS codes of rate $\frac{K}{N} \geq \frac{2}{3} + \frac{1}{N}$, ASD decoding using the bit-level MAS will succeed (i.e., the transmitted codeword is on the list) if

$$3\nu_b + e_b < \frac{3}{2}(N - K + 1) \tag{10}$$

where e_b is the number of bit-level erasures and ν_b is the number of bit-level errors in unerased locations. We can choose an appropriate distortion measure according to the following proposition which is a natural extension of Proposition 1 in the symbol level.

Proposition 3: If we choose the bit-level *letter-by-letter* distortion measure $\delta : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{R}_{\geq 0}$ as follows

$$\delta(0,0) = 1, \quad \delta(0,1) = 3,$$
$$\delta(1,0) = 1, \quad \delta(1,1) = 0,$$

then the condition (10) becomes

$$d(b^n, \hat{b}^n) < \frac{3}{2}\left(N - K + 1\right). \tag{11}$$

Proof: The condition (10) can be seen to be equivalent to

$$\frac{2}{3} d(b^n, \hat{b}^n) < N - K + 1$$

using the same reasoning as in Proposition 1. The results then follows right away. ■

Remark 6: We refer the multiple-decoding of bit-level ASD as m-bASD.

B. Symbol-level ASD case

In this subsection, we try to convert the condition for successful ASD decoding in general to the form that suits our goal. We will also determine which multiplicity assignment schemes allow us to do so.

Definition 5: (Multiplicity type) Consider a positive integer $\ell \leq m$ where m is the number of elements in $\mathbb{F}^m$. For some codeword position, let us assign multiplicity m_j to the j-th most likely symbol for $j = 1, 2, \ldots, \ell$. The remaining entries in the column are zeros by default. We call the sequence, $(m_1, m_2, \ldots, m_\ell)$, the column *multiplicity type* for "top-ℓ" decoding.

First, we notice that a choice of multiplicity types in ASD decoding at each codeword position has the similar meaning to a choice of erasure decisions in the conventional errors-and-erasures decoding. However, in ASD decoding we are more flexible and may have more types of erasures. For example, assigning multiplicity zero to all the symbols (all-zero multiplicity type) at codeword position i is similar to erasing that position. Assigning the maximum multiplicity μ to one symbol corresponds to the case when we choose that symbol as the hard-decision one. Hence, with some abuse of terminology, we also use the term (generalized) erasure pattern $\hat{x}^N$ for the multiplicity assignment scheme in the ASD context. Each erasure-letter x_i gives the multiplicity type for the corresponding column of the multiplicity matrix $\mathbf{M}$.

Definition 6: (Error patterns and erasure patterns for ASD decoding) Consider a MAS with T multiplicity types. Let $\hat{x}^N \in \{1, 2 \ldots, T\}^N$ be an erasure pattern where, at index i, $x_i = j$ implies that multiplicity type j is used at column i of the multiplicity matrix $\mathbf{M}$. Notice that the definition of an error pattern $x^N \in \mathbb{Z}_{\ell+1}^N$ in Definition 3 applies unchanged here.

Remark 7: In our method, we generally choose an appropriate integer a in Condition 2 and design a distortion measure corresponding to the chosen a so that the condition for successful ASD decoding can be converted to the form where distortion is less than a fixed threshold. The following definition of allowable multiplicity types will lead us to the result of Lemma 1 and consequently, $a \geq \mu$, as stated in Corollary 1. Also, we want to find as many as possible multiplicity types since rate-distortion theory gives us the intuition that in general the more multiplicity types (erasure choices) we have, the better performance of multiple ASD decoding we achieve as N becomes large.

Definition 7: The set of allowable multiplicity types for "top-ℓ" decoding with maximum multiplicity μ is defined to be[6]

$$\mathcal{A}(\mu, \ell) \triangleq \left\{ (m_1, m_2, \ldots, m_\ell) \left| \begin{array}{c} \sum_{j=1}^{\ell} m_j \leq \mu, \\ \sum_{j=1}^{\ell} m_j(\mu - m_j) \leq (\mu + 1)\left(|\{j : m_j \neq 0\}| - 1\right) \min_{j : m_j \neq 0} m_j \end{array} \right. \right\}. \tag{12}$$

We take the elements of this set in an arbitrary order and label them as $1, 2, \ldots, |\mathcal{A}(\mu, \ell)|$ with the convention that the multiplicity type 1 is always $(\mu, 0, \ldots, 0)$ which assigns the whole multiplicity μ to the most likely symbol. The multiplicity type k is denoted as $(m_{1,k}, m_{2,k}, \ldots m_{\ell,k})$.

Remark 8: Multiplicity types $(0, 0, \ldots, 0), (1, 1 \ldots, 1)$ as well as any permutations of $(\mu, 0, \ldots, 0)$ and $(\lfloor \frac{\mu}{2} \rfloor, \lfloor \frac{\mu}{2} \rfloor, 0, \ldots, 0)$ are always in the allowable set $\mathcal{A}(\mu, \mu)$. We use mASD-μ to denote the proposed multiple ASD decoding using $\mathcal{A}(\mu, \mu)$.

Example 4: Consider mASD-2 where $\mu = \ell = 2$. We have $\mathcal{A}(2, 2) = \{(2, 0), (1, 1), (0, 2), (0, 0)\}$ which comprises four allowable multiplicity types for "top-2" decoding as follows: the first is $(2, 0)$ where we

[6] We use the convention that $\min_{j : m_j \neq 0} m_j = 0$ if $\{j : m_j \neq 0\} = \emptyset$.

assign multiplicity 2 to the most likely symbol $y_{i,1}$, the second is $(1,1)$ where we assign equal multiplicity 1 to the first and second most likely symbols $y_{i,1}$ and $y_{i,2}$, the third is $(0,2)$ where we assign multiplicity 2 to the second most likely symbol $y_{i,2}$, and the fourth is $(0,0)$ where we assign multiplicity zero to all the symbols at index i (i.e., the i-th column of $\mathbf{M}$ is an all-zero column). We also consider a restricted set, called mASD-2a, that uses the set of multiplicity types $\{(2,0),(1,1),(0,0)\}$.

Example 5: Consider mASD-3. In this case, the allowable set $\mathcal{A}(3,3)$ consists of all the permutations of $(3,0,0),(0,0,0),(1,1,0),(2,1,0),(1,1,1)$. We can see that the set $\mathcal{A}(3,2)$ consists of all permutations of $(3,0),(2,1),(1,1),(0,0)$ and $|\mathcal{A}(3,2)| < |\mathcal{A}(3,3)|$.

From now on, we assume that only allowable multiplicity types are considered throughout most of the paper. With that setting in mind, we can obtain the following lemmas and theorems.

Lemma 1: Consider a MAS(μ,ℓ) for "top-ℓ" ASD decoding with multiplicity matrix $\mathbf{M}$ that only uses multiplicity types in the allowable set $\mathcal{A}(\mu,\ell)$. Then, the score and the cost satisfy the following inequality:

$$2C_{\mathbf{M}} \geq (\mu+1)S_{\mathbf{M}}.$$

Proof: Let us denote $e_k = |\{i \in \{1,\ldots,N\} : \hat{x}_i = k\}|$ to count the number of positions i that use multiplicity type k for $k = 1,\ldots,T$ and notice that $\sum_{k=1}^{T} e_k = N$. We also use $\nu_{j,k} = |\{i \in \{1,\ldots,N\} : x_i \neq j, \hat{x}_i = k\}|$ to count the number of positions i that use multiplicity type k where the j-th most reliable symbol $y_{i,j}$ is incorrect for $j = 0,\ldots,\ell$ and $k = 1,\ldots,T$. The notation $\chi_{j,k} = |\{i \in \{1,\ldots,N\} : x_i = j, \hat{x}_i = k\}|$ remains the same. Notice also that

$$e_k = \sum_{j=0}^{\ell} \chi_{j,k} \quad \text{and} \quad \chi_{j,k} = e_k - \nu_{j,k}. \tag{13}$$

The score and the cost can therefore be written as

$$\begin{aligned} S_{\mathbf{M}}(\mathbf{c}) &= \sum_{j=1}^{N} M_{[c_j],j} \\ &= \sum_{k=1}^{T}\sum_{j=1}^{\ell} m_{j,k}\chi_{j,k} \qquad (14) \\ &= \mu\chi_{1,1} + \sum_{k=2}^{T}\sum_{j=1}^{\ell} m_{j,k}\chi_{j,k} \qquad (15) \\ &= \mu\left(N - \sum_{k=2}^{T} e_k - \nu_{1,1}\right) + \sum_{k=2}^{T}\sum_{j=1}^{\ell} m_{j,k}(e_k - \nu_{j,k}) \qquad (16) \end{aligned}$$

and

$$\begin{aligned} C_{\mathbf{M}} &= \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{N} M_{i,j}(M_{i,j}+1) \\ &= \frac{1}{2}\sum_{k=1}^{T} e_k \sum_{j=1}^{\ell} m_{j,k}(m_{j,k}+1) \\ &= \frac{1}{2}\mu(\mu+1)\left(N-\sum_{k=2}^{T} e_k\right) + \frac{1}{2}\sum_{k=2}^{T} e_k \sum_{j=1}^{\ell} m_{j,k}(m_{j,k}+1) \qquad (17) \end{aligned}$$

where (15) and (17) use the fact that the multiplicity type 1 is always assumed to be $(\mu, 0, \ldots, 0)$.

Hence, we obtain

$$2C_{\mathbf{M}} - (\mu+1)S_{\mathbf{M}} = \mu(\mu+1)\nu_{1,1} + \sum_{k=2}^{T}(\mu+1)\sum_{j=1}^{\ell} m_{j,k}\nu_{j,k} - \sum_{k=2}^{T} e_k \sum_{j=1}^{\ell} m_{j,k}(\mu - m_{j,k}),$$

and therefore, since μ and $\nu_{1,1}$ are non-negative, Lemma 1 holds if we can show

$$(\mu+1)\sum_{j=1}^{\ell} m_{j,k}\nu_{j,k} \geq e_k \sum_{j=1}^{\ell} m_{j,k}(\mu - m_{j,k}) \qquad (18)$$

for every $k = 2, \ldots T$.

Next, we observe that

$$(\mu+1)\sum_{j=1}^{\ell} m_{j,k}\nu_{j,k} \geq (\mu+1)\left(\sum_{j:m_{j,k}\neq 0} \nu_{j,k}\right) \min_{j:m_{j,k}\neq 0} m_{j,k} \qquad (19)$$

and

$$\begin{aligned} \sum_{j:m_{j,k}\neq 0} \nu_{j,k} &= \sum_{j:m_{j,k}\neq 0} (e_k - \chi_{j,k}) \qquad (20) \\ &= e_k|\{j : m_{j,k} \neq 0\}| - \sum_{j:m_{j,k}\neq 0} \chi_{j,k} \\ &\geq e_k(|\{j : m_{j,k} \neq 0\}| - 1) \qquad (21) \end{aligned}$$

where (20) follows from (13) and (21) follows from

$$\sum_{j:m_{j,k}\neq 0} \chi_{j,k} \leq \sum_{j=0}^{\ell} \chi_{j,k} = e_k.$$

From (19) and (21), we have

$$(\mu+1)\sum_{j=1}^{\ell} m_{j,k}\nu_{j,k} \geq e_k(\mu+1)(|\{j : m_{j,k} \neq 0\}| - 1) \min_{j:m_{j,k}\neq 0} m_{j,k} \qquad (22)$$

and this motivates our definition of allowable multiplicity types.

Specifically, if we choose $\{m_{1,k}, m_{2,k}, \ldots, m_{\ell,k}\}$ in the allowable set $\mathcal{A}(\mu,\ell)$, defined in (12), then by combining with (22), we obtain (18) and this completes the proof. ■

Corollary 1: With the setting as in Lemma 1, the integer a in Condition 2 must satisfy $a \geq \mu$.

Proof: From $(a+1)\left[S_{\mathbf{M}} - \frac{a}{2}(K-1)\right] > C_{\mathbf{M}}$ and $S_{\mathbf{M}} \leq (a+1)(K-1)$ in (8) and (9), we have

$$\begin{aligned}(a+1)S_{\mathbf{M}} - C_{\mathbf{M}} &> \frac{1}{2}a(a+1)(K-1)\\ &\geq \frac{1}{2}aS_{\mathbf{M}}\end{aligned}$$

and this implies that

$$2C_{\mathbf{M}} < (a+2)S_{\mathbf{M}}. \tag{23}$$

But, Lemma 1 states that $2C_{\mathbf{M}} \geq (\mu+1)S_{\mathbf{M}}$. Combining this with (23) gives a contradiction unless $a > \mu - 1$. ■

In Condition 2, if we carefully design a distortion measure then for every $a \geq \mu$, the first constraint (8) can be equivalently converted to the form where distortion is smaller than a fixed threshold.

Theorem 1: Consider an (N,K) RS code and a MAS(μ,ℓ) for "top-ℓ" decoding with multiplicity matrix $\mathbf{M}$ that only uses T multiplicity types in the allowable set $\mathcal{A}(\mu,\ell)$. Consider an arbitrary integer $a \geq \mu$. Let $\delta_a : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}_{\geq 0}$, where in this case $\mathcal{X} = \mathbb{Z}_{\ell+1}$ and $\hat{\mathcal{X}} = \mathbb{Z}_{T+1} \setminus \{0\}$, be a *letter-by-letter* distortion measure defined by $\delta_a(x,\hat{x}) = [\Delta_a]_{x,\hat{x}}$, where Δ_a is the $(\ell+1) \times T$ matrix[7]

$$\Delta_a = \begin{pmatrix} \rho_{1,a} & \rho_{2,a} & \cdots & \rho_{T,a} \\ \rho_{1,a} - \frac{2m_{1,1}}{a} & \rho_{2,a} - \frac{2m_{1,2}}{a} & \cdots & \rho_{T,a} - \frac{2m_{1,T}}{a} \\ \rho_{1,a} - \frac{2m_{2,1}}{a} & \rho_{2,a} - \frac{2m_{2,2}}{a} & \cdots & \rho_{T,a} - \frac{2m_{2,T}}{a} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{1,a} - \frac{2m_{\ell,1}}{a} & \rho_{2,a} - \frac{2m_{\ell,2}}{a} & \cdots & \rho_{T,a} - \frac{2m_{\ell,T}}{a} \end{pmatrix} \tag{24}$$

with

$$\rho_{k,a} = \frac{\mu(2a+1-\mu)}{a(a+1)} + \sum_{j=1}^{\ell} \frac{m_{j,k}(m_{j,k}+1)}{a(a+1)}$$

for $k = 1, \ldots, T$. Then, the equation (8) in Condition 2 is equivalent to

$$d(x^N, \hat{x}^N) < \frac{\mu(2a+1-\mu)}{a(a+1)}N - K + 1 \triangleq D_a,$$

and it is easy to verify that $D_\mu = N - K + 1$.

[7] The first column of Δ_a is $[\frac{2\mu}{a}, 0, \frac{2\mu}{a}, \frac{2\mu}{a}, \ldots, \frac{2\mu}{a}]^T$ since multiplicity type 1 is always chosen to be $(\mu, 0, 0, \ldots, 0)$.

Proof: First, we show that Δ_a consists of non-zero entries. It suffices to show that $\rho_{k,a} \geq \frac{2m_{j,k}}{a}$ for all $j = 1, \ldots, \ell$ and $k = 1, \ldots, T$, i.e.,

$$\mu(2a+1-\mu) + \sum_{j'=1}^{\ell} m_{j',k}(m_{j',k}+1) \geq 2m_{j,k}(a+1)$$

which is equivalent to

$$2(a+1)(\mu - m_{j,k}) + \sum_{j'=1}^{\ell} m_{j',k}(m_{j',k}+1) - \mu(\mu+1) \geq 0. \tag{25}$$

This is true since the left hand side of (25) is at least

$$2(\mu+1)(\mu - m_{j,k}) + m_{j,k}(m_{j,k}+1) - \mu(\mu+1) = (\mu - m_{j,k})(\mu + 1 - m_{j,k}) \geq 0.$$

With the same $e_k, \nu_{j,k}, \chi_{j,k}$ as defined in the proof of Lemma 1 and the chosen distortion matrix Δ_a, we have

$$\begin{aligned} d(x^N, \hat{x}^N) &= \sum_{k=1}^{T} \left(\sum_{j=1}^{\ell} \left(\rho_{k,a} - \frac{2m_{j,k}}{a} \right) \chi_{j,k} + \rho_{k,a}\chi_{0,k} \right) \\ &= \sum_{k=1}^{T} \left(\rho_{k,a} \sum_{j=0}^{\ell} \chi_{j,k} - 2\sum_{j=1}^{\ell} \frac{m_{j,k}}{a}\chi_{j,k} \right) \\ &= \sum_{k=1}^{T} \left(\rho_{k,a} e_k - 2\sum_{j=1}^{\ell} \frac{m_{j,k}}{a}\chi_{j,k} \right). \end{aligned}$$

Noting that the first column of Δ_a is always $[\frac{2\mu}{a}, 0, \frac{2\mu}{a}, \frac{2\mu}{a}, \ldots, \frac{2\mu}{a}]^T$ and $\nu_{1,1} = e_1 - \chi_{1,1}$, we obtain

$$d(x^N, \hat{x}^N) = \frac{2\mu}{a}\nu_{1,1} + \sum_{k=2}^{T} \rho_{k,a} e_k - 2\sum_{k=2}^{T}\sum_{j=1}^{\ell} \frac{m_{j,k}}{a}\chi_{j,k}. \tag{26}$$

Next, one can see that (8) can be rewritten as

$$\frac{2S_{\mathbf{M}}}{a} - K + 1 > \frac{2C_{\mathbf{M}}}{a(a+1)}$$

which, by substituting $S_{\mathbf{M}}$ and $C_{\mathbf{M}}$ in (16) and (17), is equivalent to

$$\frac{2\mu}{a}\left(N - \sum_{k=2}^{T} e_k - \nu_{1,1}\right) + 2\sum_{k=2}^{T}\sum_{j=1}^{\ell} \frac{m_{j,k}}{a}\chi_{j,k} - K + 1 > \frac{\mu(\mu+1)}{a(a+1)}\left(N - \sum_{k=2}^{T} e_k\right) + \sum_{k=2}^{T} e_k \sum_{j=1}^{\ell} \frac{m_{j,k}(m_{j,k}+1)}{a(a+1)}.$$

Equivalently, this gives

$$\left(\frac{2\mu}{a} - \frac{\mu(\mu+1)}{a(a+1)}\right)N - K + 1 > \frac{2\mu}{a}\nu_{1,1} - 2\sum_{k=2}^{T}\sum_{j=1}^{\ell} \frac{m_{j,k}}{a}\chi_{j,k} + \sum_{k=2}^{T} e_k \left(\frac{2\mu}{a} - \frac{\mu(\mu+1)}{a(a+1)} + \sum_{j=1}^{\ell} \frac{m_{j,k}(m_{j,k}+1)}{\mu(\mu+1)} \right)$$

which in turn is equivalent to

$$\frac{\mu(2a+1-\mu)}{a(a+1)}N-K+1>\frac{2\mu}{a}\nu_{1,1}+\sum_{k=2}^{T}e_k\rho_{k,a}-\frac{2}{a}\sum_{k=2}^{T}\sum_{j=1}^{\ell}m_{j,k}\chi_{j,k}. \tag{27}$$

Finally, combining (26) and (27) gives the proof. ■

Example 6: Consider mASD-2 for $a=\mu=2$. In this case, the distortion matrix is

$$\Delta=\begin{pmatrix} 2 & 5/3 & 2 & 1 \\ 0 & 2/3 & 2 & 1 \\ 2 & 2/3 & 0 & 1 \end{pmatrix}. \tag{28}$$

However, Condition 2 also requires the second constraint (9) to be satisfied. In addition, we need to choose an integer $a\geq\mu$ in order to apply our proposed approach. Therefore, we first consider the case of high-rate RS codes where if $a=\mu$ then the satisfaction of (8) also implies the satisfaction of (9). For the case of lower-rate RS codes, we obtain a range of a and also propose a heuristic method to choose an appropriate a.

1) High-rate Reed-Solomon codes: In this subsection, we focus on high-rate RS codes which are usually seen in many practical applications. The high-rate constraint allows us to see that $a=\mu$ is essentially the correct choice.

Lemma 2: Consider an (N,K) RS code with rate

$$\frac{K}{N}\geq\frac{1}{N}+\frac{\mu}{\mu+1}.$$

If equation (8) is satisfied for $a=\mu$, or equivalently,

$$d(x^N,\hat{x}^N)<N-K+1$$

under the distortion measure Δ_μ then whole Condition 2 is satisfied and the transmitted codeword will be therefore on the list.

Proof: Suppose (8) is satisfied for $a=\mu$, i.e.,

$$S_{\mathbf{M}}>\frac{C_{\mathbf{M}}}{\mu+1}+\frac{\mu}{2}(K-1). \tag{29}$$

We will show that

$$\mu(K-1)<S_{\mathbf{M}} \tag{30}$$

$$\leq(\mu+1)(K-1) \tag{31}$$

and, therefore, both (8) and (9) in Condition 2 are satisfied for $a=\mu$.

Firstly, using Lemma 1 we have

$$\frac{S_{\mathbf{M}}}{2} \geq S_{\mathbf{M}} - \frac{C_{\mathbf{M}}}{\mu+1}$$

and consequently, (30) is implied by (29) since

$$\frac{S_{\mathbf{M}}}{2} \geq S_{\mathbf{M}} - \frac{C_{\mathbf{M}}}{\mu+1} > \frac{\mu}{2}(K-1).$$

Secondly, note that (31) holds since

$$\begin{aligned} S_{\mathbf{M}} &= \mu\left(N - \sum_{k=2}^{T} e_k - \nu_{1,1}\right) + \sum_{k=2}^{T}\sum_{j=1}^{\ell} m_{j,k}(e_k - \nu_{j,k}) \\ &= \mu N - \mu\nu_{1,1} - \sum_{k=2}^{T}\sum_{j=0}^{\ell} m_{j,k}\nu_{j,k} - \sum_{k=2}^{T} e_k\left(\mu - \sum_{j=1}^{\ell} m_{j,k}\right) \\ &\leq \mu N \qquad (32) \\ &\leq (\mu+1)(K-1) \qquad (33) \end{aligned}$$

where (32) is obtained by dropping non-negative terms and (33) follows from the high-rate constraint $\frac{K-1}{N} \geq \frac{\mu}{\mu+1}$.

Finally, by Theorem 1, one can verify that equation (8) with $a = \mu$ is equivalent to

$$d(x^N, \hat{x}^N) < D_\mu = N - K + 1$$

under the distortion measure Δ_μ. ■

However, there are possibly other integers $a \neq \mu$ that can also satisfy Condition 2. If we consider higher-rate RS codes, as in the following theorem, then we can claim that $a = \mu$ is the only such integer.

Theorem 2: Consider an (N, K) RS code with rate

$$\frac{K}{N} \geq \frac{1}{N} + \frac{\mu(\mu+3)}{(\mu+1)(\mu+2)}.$$

The integer a in Condition 2 must satisfy $a = \mu$ and, consequently, the set of constraints (8) and (9) in Condition 2 is equivalent to

$$d(x^N, \hat{x}^N) < N - K + 1$$

under the distortion measure Δ_μ.

Proof: We first see that

$$(a+1)\left[S_{\mathbf{M}} - \frac{a}{2}(K-1)\right] > C_{\mathbf{M}}$$

in (8) implies

$$S_{\mathbf{M}} - \frac{a}{2}(K-1) > \frac{C_{\mathbf{M}}}{a+1}$$

and, with the score $S_{\mathbf{M}}$ and the cost $C_{\mathbf{M}}$ computed in (16) and (17), we obtain

$$\begin{aligned}\mu\left(N-\sum_{k=2}^{T} e_k-\nu_{1,1}\right)+\sum_{k=2}^{T}\sum_{j=1}^{\ell} m_{j,k}(e_k-\nu_{j,k})-\frac{a}{2}(K-1)&\\ > \frac{\mu(\mu+1)}{2(a+1)}\left(N-\sum_{k=2}^{T} e_k\right)+\sum_{k=2}^{T} e_k\sum_{j=1}^{\ell}\frac{m_{j,k}(m_{j,k}+1)}{2(a+1)}&.\end{aligned}$$

This gives

$$\begin{aligned}\left(\mu-\frac{\mu(\mu+1)}{2(a+1)}\right)N-\frac{a}{2}(K-1) &> \mu\nu_{1,1}+\sum_{j=2}^{T}\sum_{j=1}^{\ell}\nu_{j,k}+\sum_{k=2}^{T} e_k\left(\mu-\sum_{j=1}^{\ell} m_{j,k}+\sum_{j=1}^{\ell}\frac{m_{j,k}(m_{j,k}+1)}{2(a+1)}\right)\\ &\geq \sum_{k=2}^{T} e_k\left(\mu-\sum_{j=1}^{\ell} m_{j,k}\right) \qquad (34)\\ &\geq 0 \qquad (35)\end{aligned}$$

where (34) is obtained by dropping non-negative terms.

Combining this inequality with the high-rate constraint implies that

$$\frac{\mu(2a+1-\mu)}{a(a+1)} > \frac{K-1}{N} \geq \frac{\mu(\mu+3)}{(\mu+1)(\mu+2)}$$

which leads to $a < \mu+1$, i.e. $a \leq \mu$.

This, together with $a \geq \mu$ according to Corollary 1, leave $a=\mu$ as the only possible choice. Finally, by seeing that

$$\frac{K}{N} \geq \frac{1}{N}+\frac{\mu(\mu+3)}{(\mu+1)(\mu+2)} > \frac{1}{N}+\frac{\mu}{\mu+1}$$

and applying Lemma 2 we conclude the proof. ■

Corollary 2: When the RD approach is used, $R(D)$ is positive for $D_{\min} \leq D < D_{\max}$ and is zero for $D \geq D_{\max}$. Computing $D_{\max}$ reveals how good the distortion measure matrix is at rates close to zero (i.e., the erasure codebook has only one entry). For mASD-μ,

$$D_{\max}(\text{mASD-}\mu) = \sum_{i=1}^{N}\min_{k=2,\ldots,T}\left\{2(1-p_{i,1}), \rho_{k,\mu}-\sum_{j=1}^{\ell}\frac{m_{j,k}}{\mu}p_{i,j}\right\}$$

TABLE I

EXAMPLE RANGES OF POSSIBLE a

	RS(255,191)	RS(255,127)
$\mu = 2$	$2 \le a \le 3$	$2 \le a \le 6$
$\mu = 3$	$3 \le a \le 5$	$3 \le a \le 9$

while for mBM-ℓ,

$$D_{\max}(\text{mBM-}\ell) = \sum_{i=1}^{N} \min\{1, 2(1-p_{i,1})\}.$$

Moreover, if mASD-μ uses multiplicity type $(0,0,\dots 0)$ then $D_{\max}(\text{mASD-}\mu) \le D_{\max}(\text{mBM-}\ell)$ for every μ, ℓ.

Proof: See Appendix A. ■

Example 7: Consider mASD-2 with distortion matrix in (28). We have

$$D_{\max}(\text{mASD-2}) = \sum_{i=1}^{N} \min\left\{1, 2(1-p_{i,1}), \frac{5}{3} - \frac{2}{3}(p_{i,1}+p_{i,2})\right\}$$

which is less than or equal to $D_{\max}(\text{mBM-}\ell)$ for every ℓ. This fact can be seen in Fig. 5 which is obtained by simulation. This also predicts that, as expected, ASD decoding will be superior when R is small.

2) Lower-rate Reed-Solomon codes: Without the high-rate constraint as in Theorem 2, we may not have $a = \mu$. However, we can obtain a range for a and heuristically choose the integer a that potentially give the highest rate-distortion exponent. After that, we can also apply the algorithms proposed in Section II-C with the corresponding distortion measure Δ_a and distortion threshold D_a derived in Theorem 1.

The following lemma tells us the range of possible a.

Lemma 3: Consider an (N,K) RS code. In order to satisfy (8), one must have

$$\mu \le a \le \left\lceil \mu\theta - 1/2 + \sqrt{\mu^2\theta\,(\theta-1) + 1/4} \right\rceil - 1$$

where $\theta \triangleq \frac{N}{K-1}$.

Proof: First note that (35) holds for any (N,K). Therefore, we have

$$\mu - \frac{\mu(\mu+1)}{2(a+1)} > \frac{a(K-1)}{2N}.$$

Combining this with $a \ge \mu$ in Corollary 1, we obtain the stated result. ■

Example 8: Table I gives several example ranges of possible a for some choices of μ and RS codes.

Among possible choices of a, we are interested in choosing a that gives the largest rate-distortion exponent and therefore has a better chance to satisfy Condition 2. The following lemma can give us an insight of how to choose such an integer a.

Lemma 4: If

$$a > \frac{1}{2}\left(\sqrt{1+4\theta\mu(\mu+1)}-3\right) \tag{36}$$

where $\theta = \frac{N}{K-1}$ then starting from a, the rate-distortion exponent F_a strictly decreases until reaching zero, i.e., $F_a > F_{a+1} > F_{a+2} > \ldots \geq 0$ if rate R is fixed.

Proof: For a fixed rate R, the distortion measure Δ_{a+1} and distortion D_{a+1} yield exponent F_{a+1}. Scaling both Δ_{a+1} and D_{a+1} leaves F_{a+1} unchanged. Hence, $\frac{a+1}{a}\Delta_{a+1}$ and $\frac{a+1}{a}D_{a+1}$ also yield F_{a+1}. Next, we will show that

$$\frac{a+1}{a}\Delta_{a+1} \geq \Delta_a. \tag{37}$$

To prove (37), it suffices to show

$$\frac{a+1}{a}\rho_{k,a+1} \geq \rho_{k,a} \tag{38}$$

since

$$\frac{a+1}{a}\left(\rho_{k,a+1}-\frac{2m_{j,k}}{a+1}\right) \geq \rho_{k,a}-\frac{2m_{j,k}}{a}$$

is also equivalent to (38).

Equivalently, we need to show

$$\mu(\mu+1) \geq \sum_{j=1}^{\ell} m_{j,k}(m_{j,k}+1)$$

which is true because $\mu \geq \sum_{i=1}^{\ell} m_{j,k}$ by the definition of allowable multiplicity types.

Thus, (37) holds and, therefore, the exponent yielded by Δ_a and $\frac{a+1}{a}D_{a+1}$ is at least F_{a+1}. From (36) we have

$$\begin{aligned} D_a &= \frac{\mu(2a+1-\mu)}{a(a+1)}N-K+1 \\ &> \frac{\mu(2a+3-\mu)}{a(a+2)}N-\frac{a+1}{a}(K-1) \\ &= \frac{a+1}{a}D_{a+1}. \end{aligned}$$

Since for a fixed R, exponent F is increasing in distortion D [24, Thm 6.6.2], we know that $F_a > F_{a+1}$ where F_a is the exponent yielded by Δ_a and D_a. ■

[h]

TABLE II

EXAMPLE RANGES OF a THAT GIVES THE LARGEST EXPONENT

	RS(255,191)	RS(255,127)
$\mu = 2$	$a = 2$	$a \in \{2, 3\}$
$\mu = 3$	$a = 3$	$a \in \{3, 4\}$
$\mu = 12$	$a \in \{12, 13\}$	$12 \leq a \leq 17$

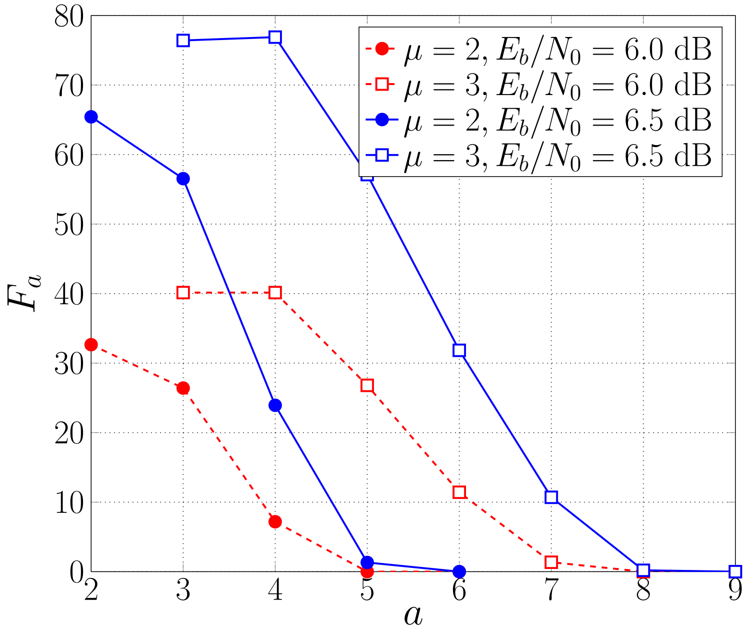

Fig. 2. Plot of exponent F_a versus a for $\mu = 2$ and $\mu = 3$ with a fixed rate $R = 6$. Simulations are conducted for the (255,127) RS code using BPSK over an AWGN channel at $E_b/N_0 = 6.0$ dB and 6.5 dB.

Corollary 3: The integer a that gives the largest exponent lies in the range

$$\mu \leq a \leq \left\lfloor \frac{1}{2}\left(\sqrt{1 + 4\theta\mu(\mu+1)} - 3\right) \right\rfloor + 1.$$

Example 9: The following Table II presents several example ranges of a that gives the largest exponent for some choices of μ and RS codes.

Remark 9: Simulation results also confirm our analysis. For example, in Fig. 2, $a = 3$ and $a = 4$ give roughly same and the largest exponents for $\mu = 3$ while $a = 2$ yields the largest exponent for $\mu = 2$. In fact, simulation results suggest that, typically, either $a = \mu$ or $a = \mu + 1$ gives the best exponent.

In Condition 2, for lower-rate RS codes, so far we have only paid attention to (8). However, it is also required that

$$a(K-1) < S_{\mathbf{M}} \leq (a+1)(K-1),$$

or equivalently

$$a+1 = \left\lceil \frac{S_{\mathbf{M}}}{K-1} \right\rceil. \tag{39}$$

While it is hard to tell exactly which a will satisfy (39) with high probability right away, we can propose a heuristic method to choose the integer a that is likely to work. We first need the following lemma.

Lemma 5: Suppose we have obtained a test-channel input-probability distribution matrix $\mathbf{Q}$ (e.g., during Step 2a or Step 2b in the proposed algorithms in Section II-C) and the set of erasure patterns for mASD is generated independently and randomly according to $\mathbf{Q}$. Then, the expected score can be computed as follows:

$$\mathbb{E}[S_{\mathbf{M}}] = \sum_{k=1}^{T} \sum_{j=1}^{\ell} \sum_{i=1}^{N} m_{j,k} p_{i,j} q_{i,k}. \tag{40}$$

Proof: The proof follows from the following equations:

$$\begin{aligned}\mathbb{E}[S_{\mathbf{M}}] &= \mathbb{E}\left[\sum_{k=1}^{T}\sum_{j=1}^{\ell} m_{j,k}\chi_{j,k}\right] \qquad (41)\\ &= \sum_{k=1}^{T}\sum_{j=1}^{\ell} m_{j,k}\mathbb{E}[\chi_{j,k}]\\ &= \sum_{k=1}^{T}\sum_{j=1}^{\ell} m_{j,k}\mathbb{E}\left[\sum_{i=1}^{N} \mathbb{1}_{\{X_i=j,\hat{X}_i=k\}}\right]\\ &= \sum_{k=1}^{T}\sum_{j=1}^{\ell}\sum_{i=1}^{N} m_{j,k}\Pr(X_i=j,\hat{X}_i=k)\\ &= \sum_{k=1}^{T}\sum_{j=1}^{\ell}\sum_{i=1}^{N} m_{j,k} p_{i,j} q_{i,k}\end{aligned}$$

where (41) is implied by (14). ■

Next, we propose a heuristic method to find the appropriate integer a to work with as follows.

Algorithm 3:

- Step 1: Start with $a = \mu$, using distortion measure Δ_a and distortion threshold D_a to get the corresponding distribution matrix $\mathbf{Q}$ as discussed above.
- Step 2: Compute the expected score $\mathbb{E}[S_{\mathbf{M}}]$ using (40). If $\left\lceil \frac{\mathbb{E}[S_{\mathbf{M}}]}{K-1} \right\rceil = a+1$ then output a and stop. If not set $a \leftarrow a+1$ and return to Step 1.

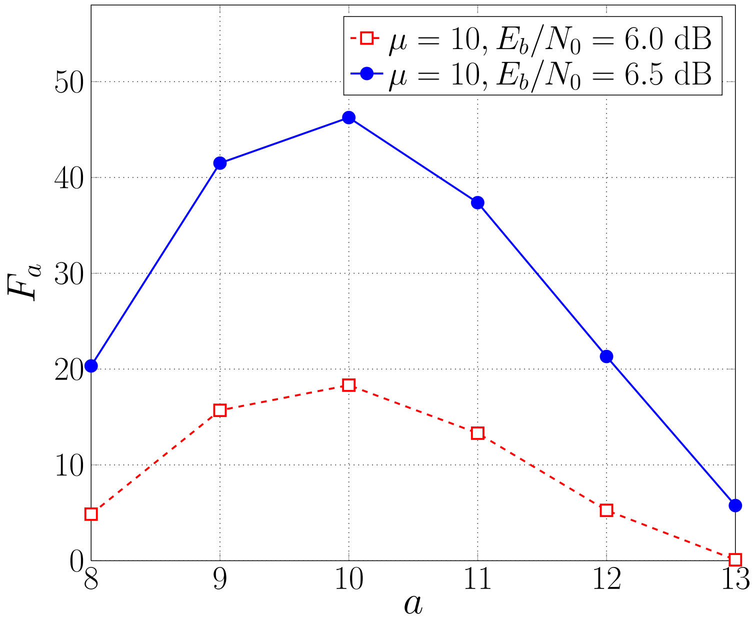

Fig. 3. Plot of exponent F_a versus a for $\mu = 10$ with a fixed rate $R = 6$. The set of multiplicity types considered is the relaxed set $\mathcal{A}_0(10, 2)$. Simulations are conducted for the (458,410) RS code over $\mathbb{F}_{2^{10}}$ using BPSK over an AWGN channel at $E_b/N_0 = 6.0$ dB and 6.5 dB.

Remark 10: In simulations with small to moderate μ, it is usually found that a is either μ or $\mu + 1$. Typically, $\frac{\mathbb{E}[S_{\mathrm{M}}]}{K-1} > \mu$ and a unit increase of a produces a small increase in $\frac{\mathbb{E}[S_{\mathrm{M}}]}{K-1}$.

Remark 11: So far, we have considered only the allowable multiplicity types in Definition 7. It is possible to obtain better performance if we relax some constraints and allow multiplicity types to be in the relaxed set

$$\mathcal{A}_0(\mu, \ell) \triangleq \left\{ (m_1, m_2, \ldots, m_\ell) \middle| \; \textstyle\sum_{j=1}^{\ell} m_j \leq \mu \; \right\}.$$

In this case, some theoretical results, e.g., results in Lemma 1 and Theorem 2, do not hold. However, this modification combined with the heuristic method above can improve the decoding performance, especially with large μ. Specifically, we consider mASD$_0$-μ which denotes our proposed multiple ASD decoding algorithm that only uses multiplicity types $(0, 0)$ and(m_1, m_2) of the form $m_1 + m_2 = \mu$. These multiplicity types form a subset of $\mathcal{A}_0(\mu, 2)$. The choice of $\ell = 2$ is suggested by observations that top-2 decoding performs almost as good as top-ℓ decoding for $\ell > 2$. The integer a used in mASD$_0$-μ is found through the heuristic method. In Fig. 3, simulations are conducted for the (458,410) RS code using BPSK over an AWGN channel. For $\mu = 10$, it can again be observed that $a = \mu$ gives the best exponent. More simulation results of this heuristic method can be seen in Section VII.

V. Closed-Form Analysis of RD and RDE Functions for Some Distortion Measures

A. Closed-form RD function

For some simple distortion measures, we can compute the RD functions analytically in closed form. First, we observe an error pattern as a sequence of i.n.d. random source components. Then, we compute the component RD functions at each index of the sequence and use convex optimization techniques to allocate the total rate and distortion to various components. This method converges to the solution faster than the numerical method in Section III. The following two theorems describe how to compute the RD functions for the simple distortion measures of Proposition 1 and 3.

Lemma 6: Consider a binary source X where $\Pr(X=1)=p$ and $\Pr(X=0)=1-p$. With the distortion measure in (2), the rate-distortion function for this source is[8]

$$R(D) = [H(p) - H(D+p-1)]^+ .$$

Proof: See Appendix B. ■

Theorem 3: (Conventional errors-and-erasures "mBM-1" decoding) Let $p_{i,1} \triangleq \Pr(X_i=1)$ for $i = 1,\ldots,N$. The overall rate-distortion function is given by

$$R(D) = \sum_{i=1}^{N} \left[H(p_{i,1}) - H(\tilde{D}_i) \right]^+$$

where $\tilde{D}_i \triangleq D_i + p_{i,1} - 1$ and $\tilde{D}_i$ can be found be a reverse water-filling procedure (see [20, Theorem 13.3.3]):

$$\tilde{D}_i = \begin{cases} \lambda & \text{if } \lambda < \min\{p_{i,1}, 1-p_{i,1}\} \\ \min\{p_{i,1}, 1-p_{i,1}\} & \text{otherwise} \end{cases}$$

where λ should be chosen so that

$$\sum_{i=1}^{N} \tilde{D}_i = D + \sum_{i=1}^{N} p_{i,1} - N.$$

The $R(D)$ function can be achieved by the test-channel input-probability distribution

$$q_{i,0} \triangleq \Pr(\hat{X}_i = 0) = \frac{1 - p_{i,1} - \tilde{D}_i}{1 - 2\tilde{D}_i}$$

and

$$q_{i,1} \triangleq \Pr(\hat{X}_i = 1) = \frac{p_{i,1} - \tilde{D}_i}{1 - 2\tilde{D}_i}.$$

Proof: See Appendix C. ■

[8] The binary entropy function is $H(u) \triangleq -u \log u - (1-u)\log(1-u)$.

Theorem 4: (Bit-level ASD “m-bASD” decoding) Let $r_{i,1} \triangleq \Pr(B_i = 1)$ and $r_{i,0} \triangleq \Pr(B_i = 0)$ for $i = 1, \ldots, n$. The overall rate-distortion function in m-bASD scheme is given by

$$R(D) = \sum_{i=1}^{n} [R_i(\lambda)]^+$$

where

$$R_i(\lambda) = H(r_{i,1}) - H\left(\frac{1+\lambda}{1+\lambda+\lambda^2}\right) + \left(r_{i,1} - \frac{1+\lambda}{1+\lambda+\lambda^2}\right) H\left(\frac{\lambda}{1+\lambda}\right)$$

and the distortion component D_i is given by

$$D_i = \begin{cases} \frac{1+2\lambda+3\lambda^2}{1+\lambda+\lambda^2} - r_{i,1}\frac{1+2\lambda}{1+\lambda} & \text{if } R_i(\lambda) > 0 \\ \min\{1, 3(1-r_{i,1})\} & \text{otherwise} \end{cases}$$

where $\lambda \in (0,1)$ should be chosen so that $\sum_{i=1}^{n} D_i = D$. The $R(D)$ function can be achieved by the following test-channel input-probability distribution

$$s_{i,0} \triangleq \Pr(\hat{B}_i = 0) = \frac{(1+\lambda) - r_{i,1}(1+\lambda+\lambda^2)}{1-\lambda^2}$$

and

$$s_{i,1} \triangleq \Pr(\hat{B}_i = 1) = \frac{r_{i,1}(1+\lambda+\lambda^2) - \lambda(1+\lambda)}{1-\lambda^2}.$$

Sketch of proof: With the distortion measure in (3), using the method in [26, Chapter 2] we can compute the rate-distortion function components

$$R_i(\lambda_i) = H(r_{i,1}) - H\left(\frac{1+\lambda_i}{1+\lambda_i+\lambda_i^2}\right) + \left(r_{i,1} - \frac{1+\lambda_i}{1+\lambda_i+\lambda_i^2}\right) H\left(\frac{\lambda_i}{1+\lambda_i}\right)$$

where λ_i is a Lagrange multiplier such that

$$D_i = \frac{1+2\lambda_i+3\lambda_i^2}{1+\lambda_i+\lambda_i^2} - r_{i,1}\frac{1+2\lambda_i}{1+\lambda_i}$$

for each bit index i. Then, the Kuhn-Tucker conditions define the overall rate allocation using the similar argument as in the proof of Theorem 3. ■

B. Closed-form RDE function

In this subsection, we consider the case mBM-1 whose distortion measure is given in (2). We study the setup that RS codewords defined over Galois field $\mathbb{F}_m$ are transmitted over the m-ary symmetric channel (m-SC) which for each parameter p can be modeled as

$$\Pr(r|c) = \begin{cases} p & \text{if } r = c \\ (1-p)/(m-1) & \text{if } r \neq c \end{cases}.$$

Here, c (resp. r) is the transmitted (resp. received) symbol and $r, c \in \mathbb{F}_m$. For this channel model, we restrict our attention to the range of p where the received symbol is the most-likely (i.e., $p > (1-p)/(m-1)$). Therefore, at each index i of the codeword, the hard-decision is also the received symbol and then it is correct with probability p. Thus, we have $p_{i,1} = \Pr(X_i = 1) = p$ for every index i of the error pattern x^N. That means, in this context we have a source x^N with i.i.d. binary components x_i. Since the components x_i's are i.i.d, we can treat each x_i as a binary source X with $\Pr(X = 1) = p$ and first compute the RDE function for this source X as given by an analysis in Appendix D. Based on this analysis, we obtain the following lemmas and theorems for the mBM-1 decoding algorithm of RS codes over an m-SC channel.

Lemma 7: Let $h(u) = H(u) - H(u + D - 1)$ map $u \in \left[1 - D, 1 - \frac{D}{2}\right)$ to R. Then, the inverse mapping of h,

$$h^{-1} : (0, H(1-D)] \to \left[1 - D, 1 - \frac{D}{2}\right),$$

is well-defined and maps R to u.

Proof: $h(u)$ is strictly decreasing since the derivative is negative over $\left[1 - D, 1 - \frac{D}{2}\right)$. Hence, the mapping $h : \left[1 - D, 1 - \frac{D}{2}\right) \to (0, H(1-D)]$ is one-to-one. From the analysis in Appendix D, one can also see that h is onto. ∎

Theorem 5: Using mBM-1 with 2^R decoding attempts where $R \in (0, NH(1 - \frac{D}{N})]$, the maximum rate-distortion exponent that can be achieved is[9]

$$F = N\, D_{KL}\left(h^{-1}\left(\frac{R}{N}\right) \middle|\middle| p\right). \tag{42}$$

Proof: First, note that in our context where we have a source sequence x^N of N i.i.d. source components, the rate and exponent for each source component are now $\frac{R}{N}$ and $\frac{F}{N}$. From Case 3 in Appendix D and from Lemma 7, we have

$$\frac{F}{N} = D_{KL}(u||p) = D_{KL}\left(h^{-1}\left(\frac{R}{N}\right) \middle|\middle| p\right)$$

and the theorem follows. ∎

Lemma 8: Let $g(u) = D_{KL}(u||p)$ map $u \in [1 - D, p]$ to F. Then, the inverse mapping of g,

$$g^{-1} : [0, D_{KL}(1 - D \,||\, p)] \to [1 - D, p]$$

is well-defined and maps F to u.

[9] The Kullback-Leibler divergence is $D_{KL}(u||p) \triangleq u \log \frac{u}{p} + (1-u) \log \frac{1-u}{1-p}$.

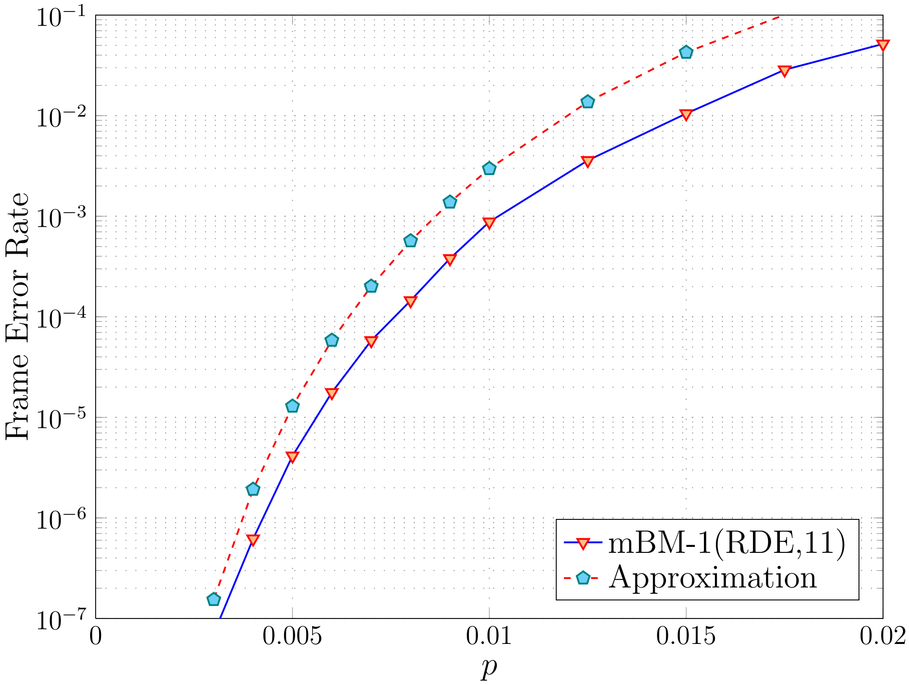

Fig. 4. Performance of mBM-1(RDE,11) and its approximation 2^{-F} where F is given in (42) for the (255,239) RS code over an m-SC(p) channel.

Proof: We first see that $g(u)$ is a strictly convex function and achieves minimum value at $u = p$ and therefore $g(u)$ is strictly decreasing over $[1-D, p]$. Thus, the mapping $g : [1-D, p] \to [0, D_{KL}(1-D\,||\,p)]$ is one-to-one. From the analysis in Appendix D, one can also see that g is onto. ■

Theorem 6: In order to achieve a rate-distortion exponent of $F \in [0, N\, D_{KL}\,(1-D\,||\,p)]$, the minimum number of decoding attempts required for mBM-1 is 2^R where

$$R = N\left[H\left(g^{-1}\left(\frac{F}{N}\right)\right) - H\left(g^{-1}\left(\frac{F}{N}\right) + \frac{D}{N} - 1\right)\right]^{+}.$$

Proof: We also note that the rate, distortion and exponent for each source component are $\frac{R}{N}$, $\frac{D}{N}$ and $\frac{F}{N}$ respectively. Combining all the cases in Appendix D, we have

$$\frac{R}{N} = \left[H\left(g^{-1}\left(\frac{F}{N}\right)\right) - H\left(g^{-1}\left(\frac{F}{N}\right) + \frac{D}{N} - 1\right)\right]^{+}$$

and the theorem follows. ■

Remark 12: In Fig. 4, we simulate the performance of mBM-1(RDE,11) for the (255,239) RS code over an m-SC channel. One curve reflects the simulated frame-error rate (FER) and the other is the approximation derived from 2^{-F} where F is given in (42) with $R = 11$.

VI. Some Extensions

A. *Erasure patterns using covering codes*

The RD framework we use is most suitable when $N \to \infty$. For a finite N, choosing random codes for only a few LRPs can be risky. We can instead use good covering codes to handle these LRPs. In the scope of covering problems, one can use an ℓ-ary t_c-covering code (e.g., a perfect Hamming or Golay code) with covering radius t_c to cover the whole space of ℓ-ary vectors of the same length. The covering may still work well if the distortion measure is close to, but not exactly equal to the Hamming distortion. The method of using covering codes in the LRPs was proposed earlier in [36] to choose the test patterns in iterative bounded distance decoding algorithms for binary linear block codes.

In order take care of up to the ℓ most likely symbols at each of the n_c LRPs of an (N, K) RS, we consider an (n_c, k_c) ℓ-ary t_c-covering code whose codeword alphabet is $\mathbb{Z}_{\ell+1} \setminus \{0\} = \{1, 2, \ldots, \ell\}$. Then, we give a definition of the (generalized) error patterns and erasure patterns for this case. In order to draw similarities between this case and the previous cases, we still use the terminology "generalized erasure pattern" and shorten it to erasure pattern even if errors-only decoding is used. For errors-only decoding, Condition 1 for successful decoding becomes

$$\nu < \frac{1}{2}(N - K + 1).$$

Definition 8: (Error patterns and erasure patterns for errors-only decoding) Let us define $x^N \in \mathbb{Z}_{\ell+1}^N$ as an error pattern where, at index i, $x_i = j$ implies that the j-th most likely symbol is correct for $j \in \{1, 2, \ldots \ell\}$, and $x_i = 0$ implies none of the first ℓ most likely symbols is correct. Let $\hat{x}^N \in \{1, 2, \ldots, \ell\}^N$ be an erasure pattern where, at index i, $\hat{x}_i = j$ implies that the j-th most likely symbol is chosen as the hard-decision symbol for $j \in \{1, 2, \ldots, \ell\}$.

Proposition 4: If we choose the *letter-by-letter* distortion measure $\delta : \mathbb{Z}_{\ell+1} \times \mathbb{Z}_{\ell+1} \setminus \{0\} \to \mathbb{R}_{\geq 0}$ defined by $\delta(x, \hat{x}) = [\Delta]_{x,\hat{x}}$ in terms of the $(\ell + 1) \times \ell$ matrix

$$\Delta = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 0 \end{pmatrix} \tag{43}$$

then the condition for successful errors-only decoding then becomes

$$d(x^N, \hat{x}^N) < \frac{1}{2}(N - K + 1). \tag{44}$$

Proof: It follows directly from

$$d(x^N, \hat{x}^N) = \sum_{k=1}^{\ell} \sum_{j=0, j\neq k}^{\ell} \chi_{j,k} = \nu.$$

■

Remark 13: If we delete the first row which corresponds to the case where none of the first ℓ most likely symbols is correct then the distortion measure is exactly the Hamming distortion.

Split covering approach: We can break an error pattern x^N into two sub-error patterns $x^{LRPs} \triangleq x_{\sigma(1)}x_{\sigma(2)}\dots x_{\sigma(n_c)}$ of n_c least reliable positions and $x^{MRPs} \triangleq x_{\sigma(n_c+1)}\dots x_{\sigma(N)}$ of $N - n_c$ most reliable positions. Similarly, we can break an erasure pattern $\hat{x}^N$ into two sub-erasure patterns $\hat{x}^{LRPs} \triangleq \hat{x}_{\sigma(1)}\hat{x}_{\sigma(2)}\dots \hat{x}_{\sigma(n_c)}$ and $\hat{x}^{MRPs} \triangleq \hat{x}_{\sigma(n_c+1)}\dots \hat{x}_{\sigma(N)}$. Let z_{n_c} be the number of positions in the n_c LRPs where none of the first ℓ most likely symbols is correct, or

$$z_{n_c} = \left|\left\{i = 1, 2, \dots, n_c : x_{\sigma(i)} = 0\right\}\right|.$$

If we assign the set of all sub-error patterns $\hat{x}^{LRPs}$ to be an (n_c, k_c) t_c-covering code then

$$d(x^{LRPs}, \hat{x}^{LRPs}) \leq t_c + z_{n_c}$$

because this covering code has covering radius t_c. Since

$$d(x^N, \hat{x}^N) = d(x^{LRPs}, \hat{x}^{LRPs}) + d(x^{MRPs}, \hat{x}^{MRPs}),$$

in order to increase the probability that the condition (44) is satisfied we want to make $d(x^{MRPs}, \hat{x}^{MRPs})$ as small as possible by the use of the RD approach. The following proposition summarizes how to generate a set of 2^R erasure patterns for multiple runs of errors-only decoding.

Proposition 5: In each erasure pattern, the letter sequence at n_c LRPs is set to be a codeword of an (n_c, k_c) ℓ-ary t_c-covering code. The letter sequence of the remaining $N - n_c$ MRPs is generated randomly by the RD method (see Section II-C) with rate $R_{MRPs} = R - k_c \log_2 \ell$ and the distortion measure in (43). Since this covering code has ℓ^{k_c} codewords, the total rate is $R_{MRPs} + \log_2 \ell^{k_c} = R$.

Example 10: For a (7,4,3) binary Hamming code which has covering radius $t_c = 1$, we take care of the 2 most likely symbols at each of the 7 LRPs. We see that 1001001 is a codeword of this Hamming code and then form erasure patterns $1001001\hat{x}_8\hat{x}_9\dots\hat{x}_n$ with assumption that the positions are written in increasing reliability order. The 2^{R-4} sub-erasure patterns $\hat{x}_8\hat{x}_9\dots\hat{x}_n$ are generated randomly using the RD approach with rate $(R - 4)$.

Remark 14: While it also makes sense to use a covering codes for the n_c LRPs of the erasure patterns and set the rest to be letter 1 (i.e., chose the most likely symbol as the hard-decision), our simulation results shows that the performance can usually be improved by using a combination of a covering code and a random (i.e., generated by the RD approach) code. More discussions are presented in Section VII.

B. A single decoding attempt

In this subsection, we investigate a special case of our proposed RDE framework when $R = 0$ (i.e., the set of erasure patterns consists of one pattern). In this case, our proposed approach is related to another line of work where one tries to design a good erasure pattern for a single BM decoding or a good multiplicity matrix for a single ASD decoding [14], [16], [15], [17]. We will see that the RDE approach for $R = 0$ is quite similar to optimizing a Chernoff bound [16], [15] or using the method of types [17]. The main difference is that this approach starts from Condition 2 rather than its large multiplicity approximation.

Lemma 9: When rate $R = 0$, the distribution matrix $\mathbf{Q}$ that optimizes the RDE/RD function consists of only binary entries. Consequently, the random codebook using the proposed RDE approach (the set of erasure patterns) becomes a single deterministic pattern.

Sketch of proof: For each (s, t) pair, the total rate is the sum of N individual components as seen in Proposition 2. Therefore, the zero total rate implies all components are zero. Thus, it suffices to show that if an arbitrary rate component (denoted as R in the proof) is zero then the corresponding column of $\mathbf{Q}$ has all entries equal to 0 or 1.

For the RD case, it is well known [26, p. 27] that if $R = 0$ then the distortion is given by $D_{\max} = \min_k \sum_j p_j \delta_{jk}$ where $k^\star$ is the argument that achieves this minimum and the test-channel input distribution is

$$q_k^\star = \begin{cases} 1 & \text{if } k = k^\star \\ 0 & \text{otherwise} \end{cases}.$$

Computing the RDE for the source distribution p_j is equivalent to solving the RD problem for an appropriately tilted source distribution $\tilde{p}_j^\star$. Therefore, the above property is inherited by the RDE as well. In particular, the distortion at $R = 0$ is given by $\min_k \sum_j \tilde{p}_j^\star \delta_{jk}$ and the test-channel input distribution is supported on the singleton element that achieves this minimum.

This result can also be shown directly by solving (6) while dropping the rate constraint from (7). ■

Let $G_k(D)$ be the large deviation rate-function for the distortion when the reconstruction symbol is fixed to k. It is well-known that this can be computed using either a Chernoff bound or the method of types

[20]. Both techniques result in the same function; for $\alpha \geq 0$, it is described implicitly by

$$D(\alpha) = \frac{\sum_j p_j 2^{\alpha \delta_{j,k}} \delta_{j,k}}{\sum_{j'} p_{j'} 2^{\alpha \delta_{j',k}}},$$

$$G_k(\alpha) = \sum_j \frac{p_j 2^{\alpha \delta_{j,k}}}{\sum_{j'} p_{j'} 2^{\alpha \delta_{j',k}}} \log \frac{2^{\alpha \delta_{j,k}}}{\sum_{j'} p_{j'} 2^{\alpha \delta_{j',k}}}.$$

Theorem 7: The RDE function for $R = 0$ is equal to

$$F(0, D) = \max_k G_k(D).$$

Proof: Lemma 9 shows that the reconstruction distribution must be supported on a single element. Since the exponential failure probability for any fixed reconstruction symbol follows from a standard large-deviations analysis, the only remaining degree of freedom is which symbol to use. Choosing the best symbol maximizes the RDE. ■

Remark 15: This means that the single decoding attempt with the best error-exponent can be computed as a special case of the RDE approach. Simplifying our proposed algorithm to use the single Lagrange multiplier α leads to an algorithm that is very similar to the one proposed in [17]. It also seems unlikely that this new algorithm will provide any significant performance gains either in performance or complexity.

VII. Simulation results

In this section, we present simulation results on the performance of RS codes over an AWGN channel with either BPSK or 256-QAM as the modulation format. In all the figures, the curve labeled mBM-1 corresponds to standard errors-and-erasures BM decoding with multiple erasure patterns. For $\ell > 1$, the curves labeled mBM-ℓ correspond to errors-and-erasures BM decoding with multiple decoding trials using both erasures and the top-ℓ symbols. The curves labeled mASD-μ correspond to multiple ASD decoding trials with maximum multiplicity μ. The number of decoding attempts is 2^R where R is denoted in parentheses in each algorithm's acronym (e.g., mBM-2(RD,11) uses the RD approach with $R = 11$ while mBM-2(RDE,10) uses the RDE approach with $R = 10$). Please note that not all the algorithms listed in this section are of the same complexity unless stated explicitly.

In Fig. 5, the RD curves are shown for various algorithms using the RD approach at $E_b/N_0 = 5.2$ dB where BPSK is used. For the (255,239) RS code, the fixed threshold for decoding is $D = N - K + 1 = 17$. Therefore, one might expect that algorithms whose average distortion is less than 17 should have a frame error rate (FER) less than $\frac{1}{2}$. The RD curve allows one to estimate the number of decoding patterns required to achieve this FER. Notice that the mBM-1 algorithm at rate 0, which is very similar to conventional BM decoding, has an expected distortion of roughly 24. For this reason, the FER for

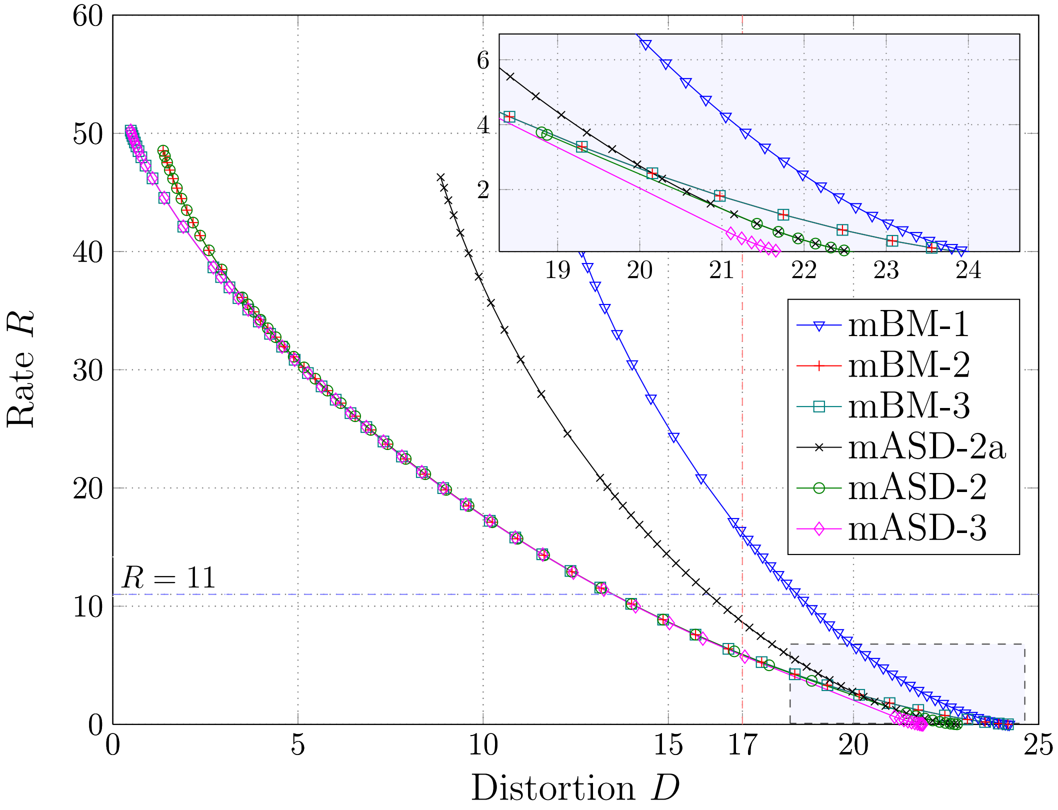

Fig. 5. A realization of RD curves at $E_b/N_0 = 5.2$ dB for various decoding algorithms for the (255,239) RS code over an AWGN channel.

conventional decoding is close to 1. The RD curve tells us that trying roughly 2^{16} (i.e., $R = 16$) erasure patterns would reduce the FER to roughly $\frac{1}{2}$ because this is where the distortion drops down to 17. Likewise, the mBM-2 algorithm using rate $R = 11$ has an expected distortion of less than 14. So we expect (and our simulations confirm) that the FER should be less than $\frac{1}{2}$.

One weakness of this RD approach is that RD describes only the average distortion and does not directly consider the probability that the distortion is greater than 17. Still, we can make the following observations from the RD curve. Even at high rates (e.g., $R \geq 5$), we see that the distortion D achieved by mBM-2 is roughly the same as mBM-3, mASD-2, and mASD-3 but smaller than mASD-2a (see Example 4) and mBM-1. This implies that, for this RS code, mBM-2 using the RD approach is no worse than the more complicated ASD based approaches for a wide range of rates (i.e., $5 \leq R \leq 35$). This is also true if the RDE approach is used as can be seen in Fig. 6 which depicts the trade-off between rate R and exponent F for various algorithms at $E_b/N_0 = 6$ dB. For this RS code, ASD based approaches

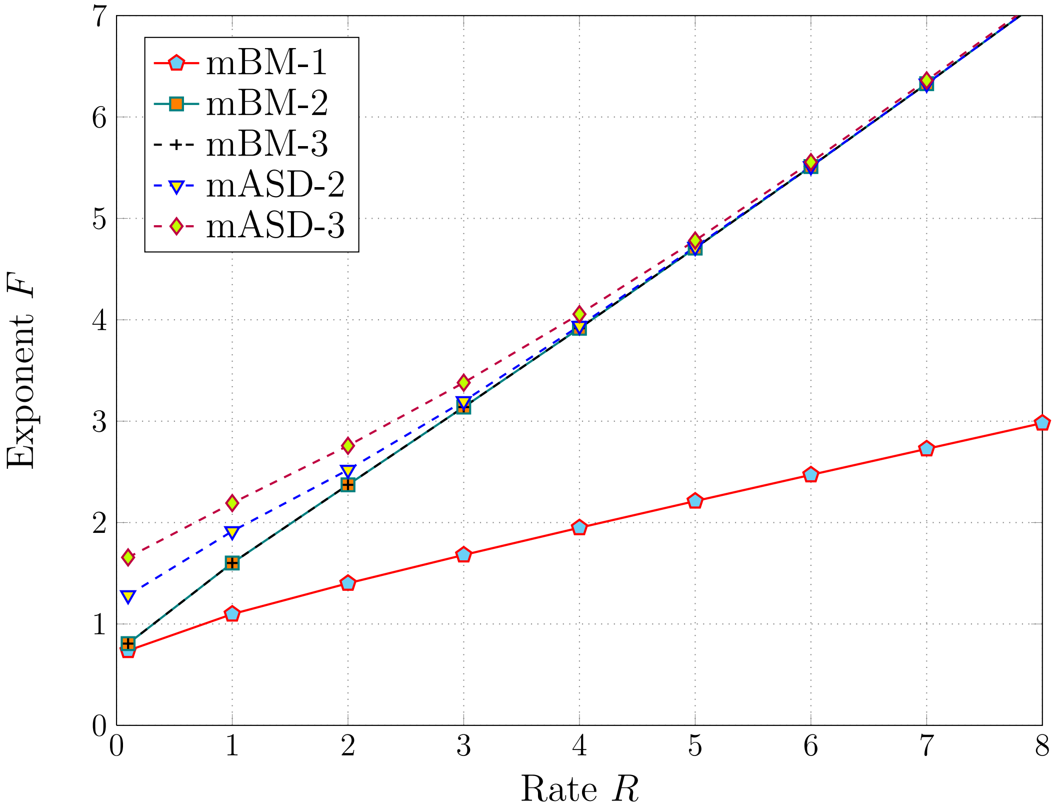

Fig. 6. A realization of RDE curves at $E_b/N_0 = 6$ dB for various decoding algorithms for the (255,239) RS code over an AWGN channel.

have a better exponent than mBM-2 at low rates (i.e., small number of decoding trials) and have roughly the same exponent for rates $R \geq 5$.

In Fig. 7, a plot of the FER versus E_b/N_0 is shown for the (255,239) RS code over an AWGN channel with BPSK as the modulation format. The conventional HDD and the GMD algorithms have modest performance since they use only one or a few decoding attempts. Choosing $R = 11$ allows us to make fair comparisons with SED(12,12). With the same number of decoding trials, mBM-2(RD,11) outperforms SED(12,12) by 0.3 dB at FER= 10^{-4}. Even mBM-2(RD,7), with many fewer decoding trials, outperforms both SED(12,12) and the KV algorithm with $\mu = \infty$. Among all our proposed algorithms using the RD approach with rate $R = 11$, the mBM2-HM74(RD,11) achieves the best performance. This algorithm uses the Hamming (7,4) covering code for the 7 LRPs and the RD approach for the remaining codeword positions. Meanwhile, small differences in the performance among mBM-2(RD,11), mBM-3(RD,11), mASD-2(RD,11), and mASD-3(RD,11) suggest that: (i) taking care of the 2 most likely symbols at each

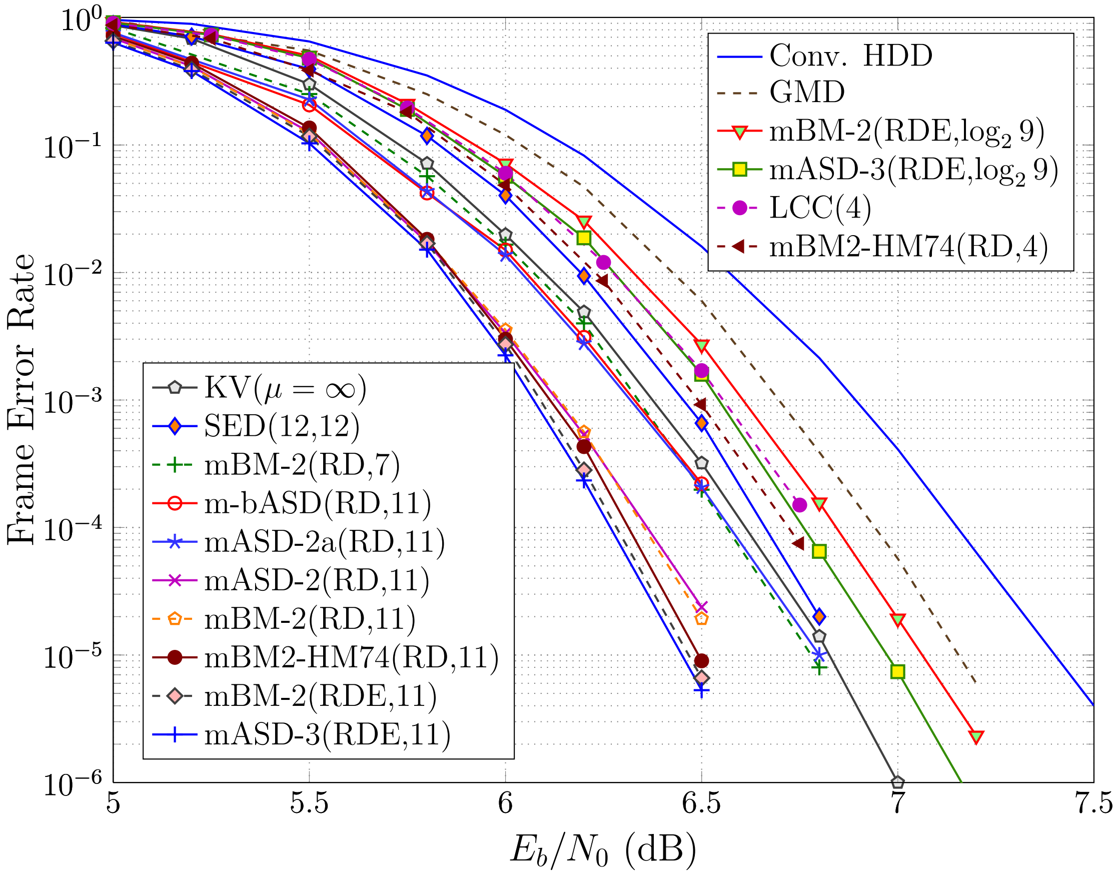

Fig. 7. Performance of various decoding algorithms for the (255,239) RS code using BPSK over an AWGN channel.

codeword position is good enough for multiple decoding of this RS code and (ii) multiple runs of errors-and-erasures decoding is generally almost as good as multiple runs of ASD decoding. Recall that this result is also correctly predicted by the RD analysis. When the RDE approach is used, mBM-2(RDE,11) still has roughly the same performance as a more complex mASD-3(RDE,11). One can also observe that these two algorithms using the RDE approach achieve better performance than mBM-2(RD,11) and mBM2-HM74(RD,11) that use the RD approach. We also simulate our proposed algorithm at $R = \log_2 9$ to compare with the GMD algorithm. While both mBM-2(RDE,$\log_2 9$) and the GMD algorithm use the same number of 9 errors-and-erasures decoding attempts, mBM-2(RDE,$\log_2 9$) yields roughly a 0.1 dB gain. The simulation results show that, at this low rate $R = \log_2 9$, mASD-3 has a larger gain over mBM-2 than at a higher rate $R = 11$. This phenomenon can be predicted in Fig. 6 where mASD-3 starts to achieve a larger exponent F at small values of R.

To compare with the Chase-type approach (LCC) used in [9], in Fig. 7 we also consider the mBM2-

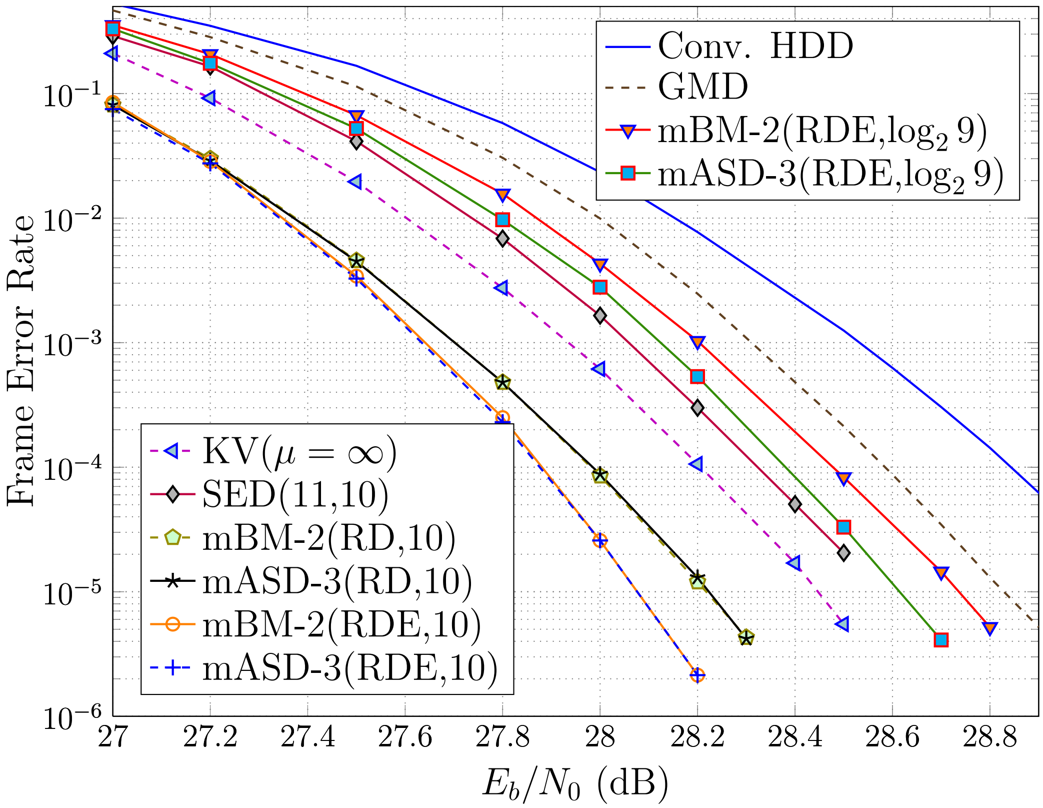

Fig. 8. Performance of various decoding algorithms for the (255,239) RS code using 256-QAM over an AWGN channel.

HM74(4) algorithm that uses the Hamming (7,4) covering code for the 7 LRPs and the hard decision pattern for the remaining codeword positions. This shows that, for the (255,239) RS code, the mBM2-HM74 achieves better performance than the LCC(4) with the same number (2^4) of decoding attempts. For the (458,410) RS code considered in Fig. 9, one can also observe that the group of algorithms that we propose have better performance than LCC(10) with the same number (2^{10}) of decoding attempts. However, the implementation complexity of LCC(10) may be lower than the algorithms proposed here due to their clever techniques that reduce the decoding complexity per trial. It is also interesting to note that the method proposed here, based on covering codes and random codebook generation, is also compatible with some of the fast techniques used by the LCC decoding.

We also performed simulations using QAM and Fig. 8 shows FER versus E_b/N_0 performance of the same (255,239) RS code transmitted over an AWGN channel with 256-QAM modulation. At FER=10^{-4}, our proposed algorithms mBM-2(RD,10) and mBM-2(RDE,10) achieve $0.3-0.4$ dB gain over SED(11,10) (with the same complexity) and also outperform KV($\mu = \infty$). At $R = 10$, mBM-2 still achieves roughly

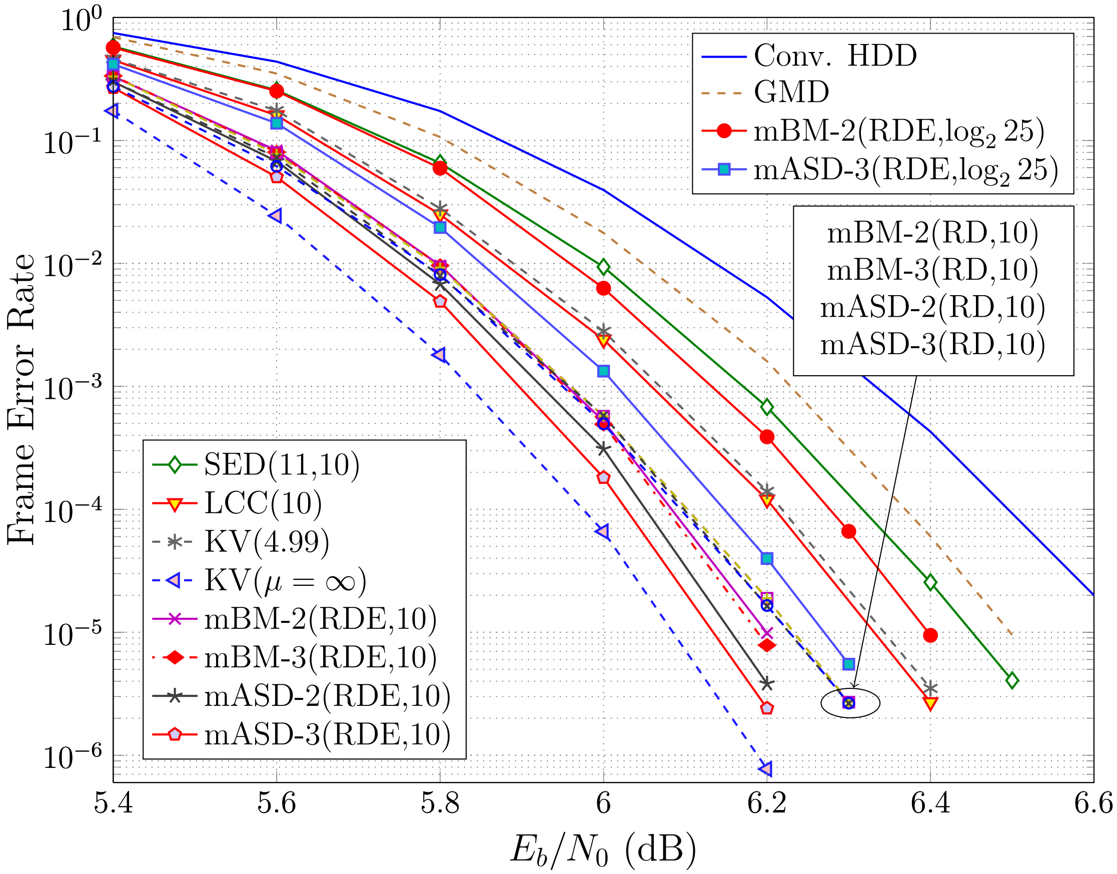

Fig. 9. Performance of various decoding algorithms for the (458,410) RS code over $\mathbb{F}_{2^{10}}$ using BPSK over an AWGN channel.

the same performance as mASD-3.

In Fig. 9, a plot of the FER versus E_b/N_0 is shown for the (458,410) RS code that has a longer block length. In this plot, BPSK is used as the modulation format and we also focus on rate $R = 10$. With algorithms that use the RD approach, mBM-2(RD,10) still has approximately the same performance as mBM-3(RD,10), mASD-2(RD,10), mASD-3(RD,10). However, when the RDE approach is employed, algorithms that run multiple ASD decoding attempts have a recognizable gain over algorithms that use multiple runs of BM decoding. The performance gain of the RDE approach (over the RD approach) is small, but can be seen easily by comparing mASD-3(RDE,10) to mASD-3(RD,10). As a reference, we also plot the performance of KV(4.99) which corresponds to the proportional KV algorithm [32] with the scaling factor 4.99.

In Fig. 10, the same setting is used as in Fig. 9. As can be seen in the figure, KV($\mu = \infty$) achieve better performance than mASD-3(RDE,10) and mBM-2(RDE,10). However, by considering higher μ,

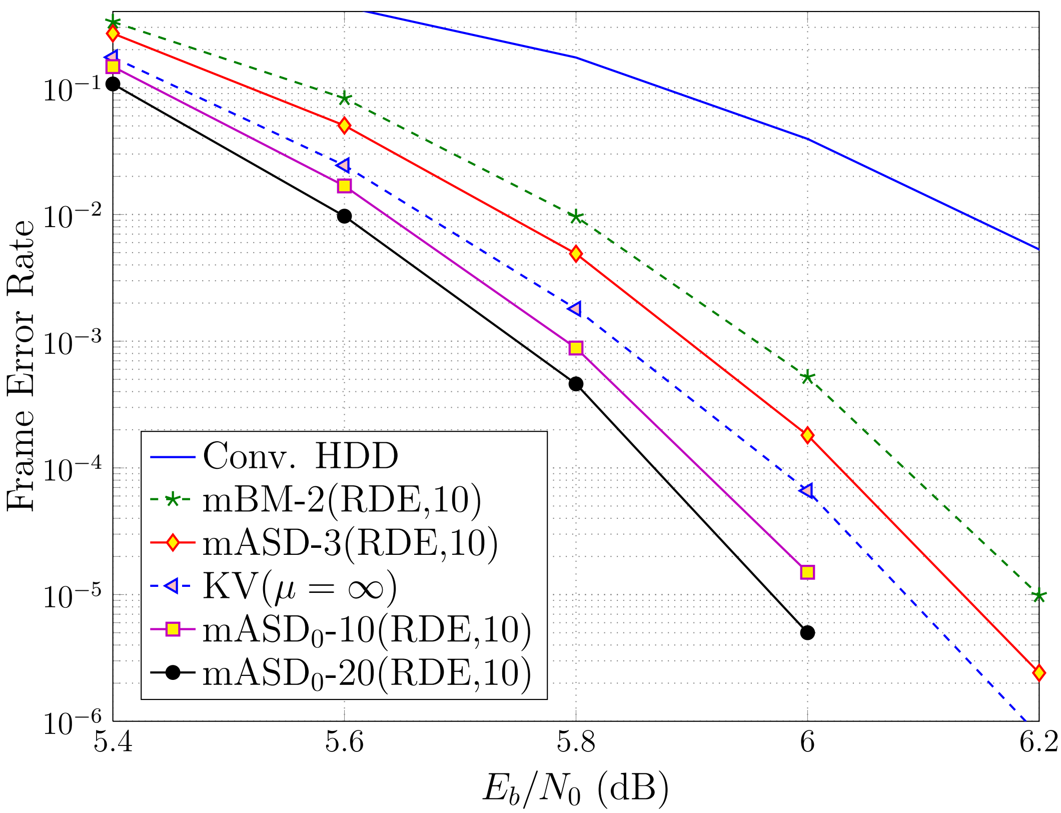

Fig. 10. Performance of various decoding algorithms for the (458,410) RS code over $\mathbb{F}_{2^{10}}$ using BPSK over an AWGN channel.

our algorithms using the heuristic method mASD$_0$-10(RDE,10) and mASD$_0$-20(RDE,10) can outperform KV($\mu = \infty$).

To target RS codes of lower rate, we also ran simulations of the (255,127) RS code over an AWGN channel with BPSK modulation and the results can be seen in Fig. 11. While mBM-2(RDE,6), mBM-2(RD,6), SED(7,6) and GMD all use the same number of about 64 errors-and-erasures decoding attempts, our proposed mBM-2 algorithms outperforms the other two algorithms. As seen in the plot, mASD-3(RDE,6) has quite a large gain over mBM-2(RD,6) which is reasonable since ASD decoding is known to perform very well compared to BM decoding with low-rate RS codes. In this figure, KV(3.99) denotes the proportional KV algorithm [32] with the scaling factor 3.99 and therefore with maximum multiplicity $\mu = 3$. While mASD-3(RDE,6) with 64 decoding attempts outperforms KV(3.99) as expected, the small gain of roughly 0.5 dB at FER=10^{-4} suggests that with low-rate RS codes, one might prefer increasing μ in a single ASD decoding attempt to running multiple ASD decoding attempts of a lower μ.

In Fig. 12, we show the FER versus E_s/N_0 performance for the (255,191) RS codes using 256-QAM.

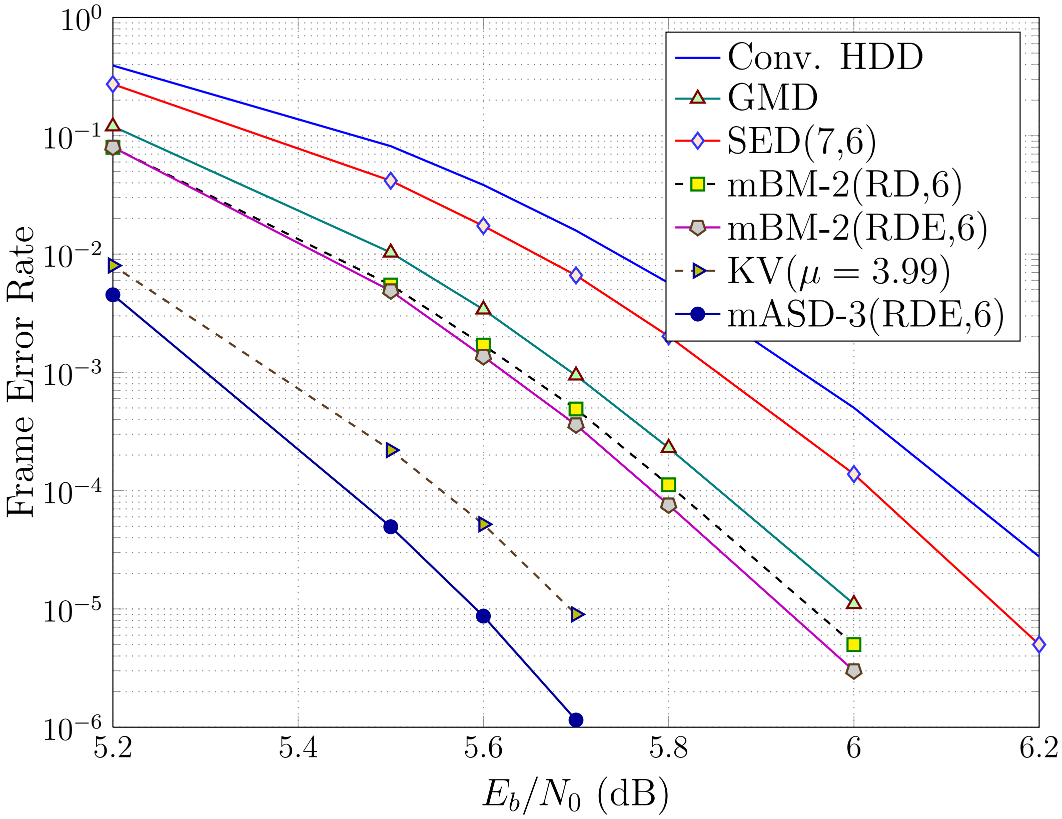

Fig. 11. Performance of various decoding algorithms for the (255,127) RS code using BPSK over an AWGN channel.

Again, our proposed algorithm mBM-2(RDE,5) performs favorably compared to SED(6,6) and GMD with the same number of about 32 errors-and-erasures decoding attempts. Under this setup, mASD-2(RDE,5) and mASD-3(RDE,5) achieve significant gains over mBM-2(RDE,5). Our proposed mASD-3(RDE,11) and mASD-3(RDE,5) algorithms have fairly the same performance as the proportional KV algorithm with the scaling factor 12.99 and 6.99, respectively.

To compare with the iterative erasure and error decoding (IEED) algorithm proposed in [8], we also conducted simulations of the (255,223) RS code over an AWGN channel using BPSK and the results are shown in Fig. 13. With the same number of about 17 errors-and-erasures decoding attempts, our proposed mBM-2(RDE,$\log_2 17$) algorithm outperforms both the GMD and 17-IEED algorithms. In fact, at FER smaller than 10^{-3}, mBM-2(RDE,$\log_2 17$) has roughly the same performance as 32-IEED which needs to use 32 decoding attempts. Meanwhile, mBM-2(RDE,5) that uses 32 decoding attempts performs as good as 112-IEED where 112 decoding attempts are required.

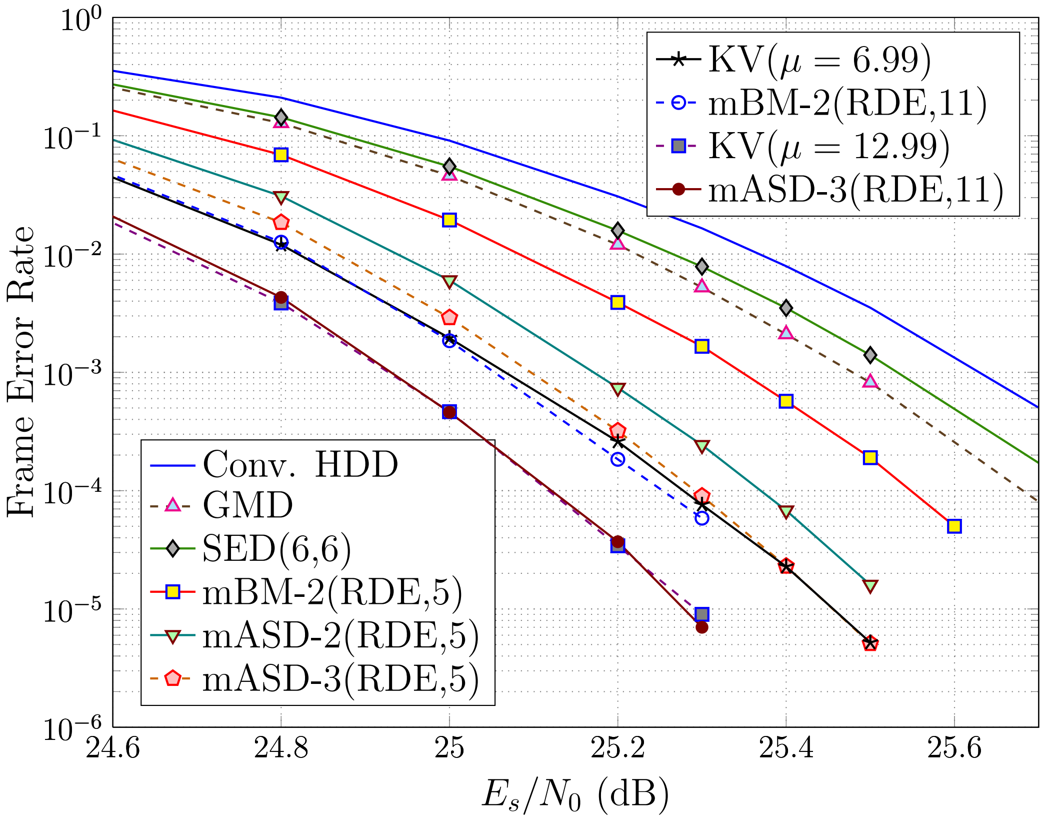

Fig. 12. Performance of various decoding algorithms for the (255,191) RS code using 256-QAM over an AWGN channel.

VIII. Conclusion

A unified framework based on rate-distortion (RD) theory has been developed to analyze multiple decoding trials, with various algorithms, of RS codes in terms of performance and complexity. An important contribution of this paper is the connection that is made between the complexity and performance (in an asymptotic sense) of these multiple-decoding algorithms and the rate-distortion of an associated RD problem. Based on this analysis, we propose two solutions; the first is based on the RD function and the second on the RD exponent (RDE). The RDE analysis shows that this approach has several advantages. Firstly, the RDE approach achieves a near optimal performance-versus-complexity trade-off among algorithms that consider running a decoding scheme multiple times (see Remark 1). Secondly, it helps estimate the error probability using exponentially tight bounds for N large enough. Further, we have shown that covering codes can also be combined with the RD approach to mitigate the suboptimality of random codes when the effective block-length is not large. As part of this analysis, we also present numerical and analytical computations of the RD and RDE functions for sequences

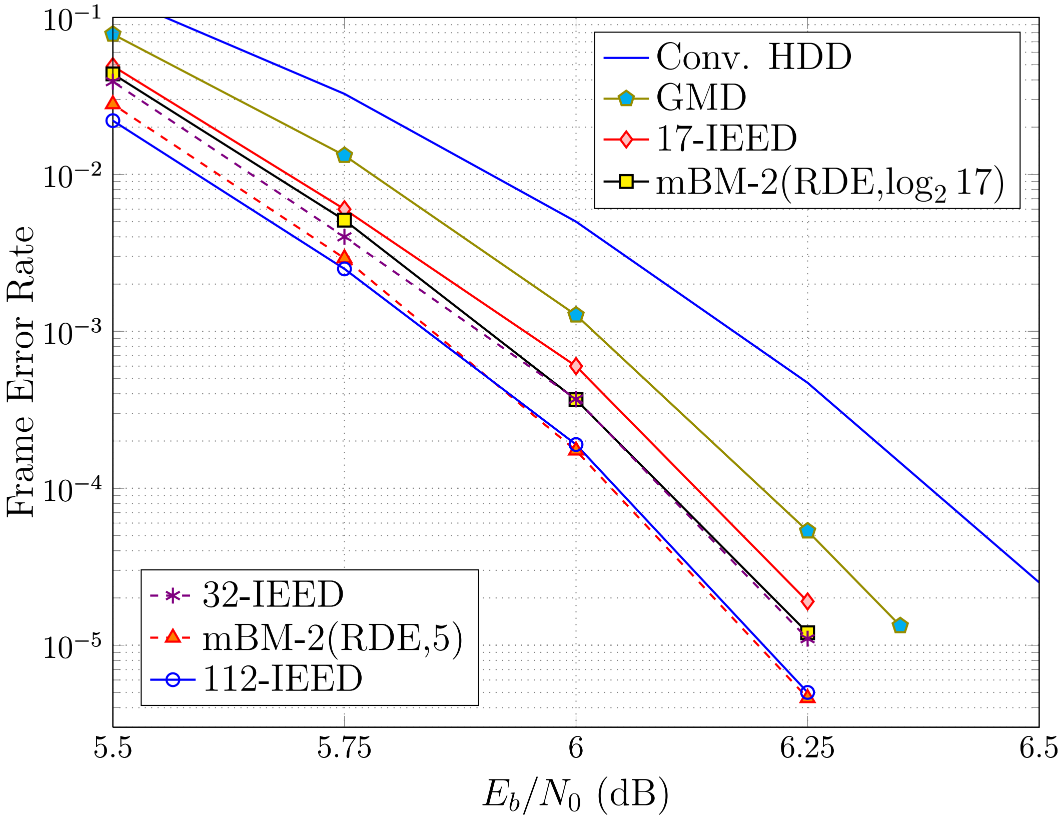

Fig. 13. Performance of various decoding algorithms for the (255,223) RS code using BPSK over an AWGN channel.

of i.n.d. sources. Finally, the simulation results show that our proposed algorithms based on the RD and RDE approaches achieve a better performance-versus-complexity trade-off than previously proposed algorithms. One key result is that, for the $(255, 239)$ RS code, multiple-decoding using the standard Berlekamp-Massey algorithm (mBM) is as good as multiple-decoding using more complex algebraic soft-decision algorithms (mASD). However, for the $(458, 410)$ RS code, the RDE approach improves the performance of mASD algorithms beyond that of mBM decoding.

Simulations results suggest an interesting conjecture that for moderate-rate RS codes, multiple ASD decoding attempts with small μ is preferred while for low-rate RS codes, a single ASD decoding with large μ may be preferred. This conjecture remains open for future research. Our future work will also focus on extending this framework to analyze multiple decoding attempts for intersymbol interference channels. In this case, it will be appropriate for the decoder to consider multiple candidate error-events during decoding. Extending the RD and RDE approaches directly to this case is not straightforward since computing the RD and RDE functions for Markov sources in the large distortion regime is still an open problem. Another interesting extension is to use clever techniques to reuse the computations from one stage of errors-and-erasures decoding to the next in order to lower the complexity per decoding trial (e.g., [9]).

Appendix A
Proof of Corollary 2

Proof: Using the formula in [26, p. 27], we have

$$D_{\max} = \sum_{i=1}^{N} \min_{k} \sum_{j=0}^{\ell} p_{i,j}\delta_{jk}.$$

For mBM-ℓ with distortion matrix in (4), we have $\sum_{j=0}^{\ell} p_{i,j}\delta_{jk} = \sum_{j\neq k} 2p_{i,j} = 2(1-p_{i,k})$ for $k \geq 1$ and $\sum_{j=0}^{\ell} p_{i,j}\delta_{j0} = \sum_{j=0}^{\ell} p_{i,j} = 1$. Therefore,

$$\begin{aligned} D_{\max}(\text{mBM-}\ell) &= \sum_{i=1}^{N} \min_{k=1,\dots\ell}\{1, 2(1-p_{i,k})\} \\ &= \sum_{i=1}^{N} \min\{1, 2(1-p_{i,1})\} \end{aligned}$$

since $p_{i,1} = \max_{k\geq 1}\{p_{i,k}\}$.

Similarly, for mASD-μ with distortion matrix Δ_μ in (24), we have

$$\begin{aligned} \sum_{j=0}^{\ell} p_{i,j}\delta_{jk} &= p_{i,0}\rho_{k,\mu} + \sum_{j=1}^{\ell} p_{i,j}\left(\rho_{k,\mu} - \frac{2m_{j,k}}{\mu}\right) \\ &= \rho_{k,\mu} - \sum_{j=1}^{\ell} \frac{m_{j,k}}{\mu} p_{i,j} \end{aligned}$$

for $k = 1, \dots, T$. Since multiplicity type 1 is always defined to be $(\mu, 0, \dots, 0)$, we have $\rho_{1,\mu} = 2$ and consequently,

$$\sum_{j=0}^{\ell} p_{i,j}\delta_{j1} = 2(1-p_{i,1}).$$

Therefore, we obtain

$$D_{\max}(\text{mASD-}\mu) = \sum_{i=1}^{N} \min_{k=2,\dots,T}\left\{2(1-p_{i,1}), \rho_{k,\mu} - \sum_{j=1}^{\ell}\frac{m_{j,k}}{\mu}p_{i,j}\right\}.$$

If mASD-μ uses multiplicity type $(0, 0, \dots 0)$ which is, for example, labeled as type T then we have

$$\rho_{T,\mu} - \sum_{j=1}^{\ell}\frac{m_{j,T}}{\mu}p_{i,j} = \rho_{T,\mu} = 1.$$

Consequently,

$$\begin{aligned} D_{\max}(\text{mASD-}\mu) &= \sum_{i=1}^{N} \min_{k=2,\ldots,T-1} \left\{ 1, 2(1-p_{i,1}), \rho_{k,\mu} - \sum_{j=1}^{\ell} \frac{m_{j,k}}{\mu} p_{i,j} \right\} \\ &\leq \sum_{i=1}^{N} \min\{1, 2(1-p_{i,1})\} \\ &= D_{\max}(\text{mBM-}\ell) \end{aligned}$$

and this completes the proof. ■

Appendix B
Proof of Lemma 6

Proof: With the notation $\bar{p} = 1-p$, according to [26, p. 27] we have

$$\begin{aligned} D_{\min} &= \bar{p} \min_k \delta_{0k} + p \min_k \delta_{1k} = 1-p \\ D_{\max} &= \min_k (\bar{p}\delta_{0k} + p\delta_{1k}) = \min\{1, 2(1-p)\}. \end{aligned}$$

The function $R(D)$ is not defined for $D < D_{\min}$ and $R(D) = 0$ for $D \geq D_{\max}$. For the case $D_{\min} \leq D < D_{\max}$, the rate-distortion function $R(D)$ is given by solving the following convex optimization problem

$$\begin{array}{rc} \min_{\mathbf{w}} & I(X;\hat{X}) \\ \text{subject to} & w_{k|j} \triangleq \Pr(\hat{X} = k | X = j) \geq 0 \;\; \forall j,k \in \{0,1\} \\ & w_{0|0} + w_{1|0} = 1 \\ & w_{0|1} + w_{1|1} = 1 \\ & \bar{p} w_{0|0} + p w_{0|1} + 2\bar{p} w_{1|0} = D \end{array}$$

where the mutual information

$$I(X;\hat{X}) = \bar{p} \sum_k w_{k|0} \log \frac{w_{k|0}}{q_k} + p \sum_k w_{k|1} \log \frac{w_{k|1}}{q_k}$$

and the test-channel input probability-distribution

$$q_k = \Pr(\hat{X} = k) = \bar{p} w_{k|0} + p w_{k|1}.$$

We then form the Lagrangian

$$J(W) = I(X;\hat{X}) + \sum_j \gamma_j (w_{0|j} + w_{1|j} - 1) + \gamma(\bar{p} w_{0|0} + p w_{0|1} + 2\bar{p} w_{1|0} - D) - \sum_{j,k} \lambda_{jk} w_{k|j}$$

and the Karush-Kuhn-Tucker (KKT) conditions become[10]

$$\begin{cases} \frac{\partial J}{\partial w_{k|j}} = 0 & \forall j,k \in \{0,1\} \\ w_{0|j} + w_{1|j} - 1 = 0 & \forall j \in \{0,1\} \\ w_{k|j}, \lambda_{jk} \geq 0 & \forall j,k \in \{0,1\} \\ \lambda_{jk} w_{k|j} = 0 & \forall j,k \in \{0,1\} \end{cases}.$$

By [26, Lemma 1, p. 32], we only need to consider the following cases.

- Case 1: $w_{0|0} = w_{0|1} = 0$. In this case, we further have $w_{1|0} = w_{1|1} = 1$. This leads to $R = 0$ and $D = 2(1-p) \geq D_{\max}$ which is a contradiction as we only consider $D \in [D_{\min}, D_{\max})$.
- Case 2: $w_{1|0} = w_{1|1} = 0$. In this case, we have $w_{0|0} = w_{0|1} = 1$. This leads to $R = 0$ and $D = 1 \geq D_{\max}$ which is also a contradiction.
- Case 3: $w_{k|j} > 0$ $\forall j,k \in \{0,1\}$. In this case, we know $\lambda_{jk} = 0$ and then, from $\frac{\partial J}{\partial w_{k|j}} = 0$, we obtain

$$\begin{aligned} \bar{p}(\log \frac{w_{k|0}}{q_k} + \delta_{0k}\gamma) + \gamma_0 = 0 \quad \forall k \in \{0,1\}, \\ p(\log \frac{w_{k|1}}{q_k} + \delta_{1k}\gamma) + \gamma_1 = 0 \quad \forall k \in \{0,1\}. \end{aligned}$$

Equivalently, we have

$$\begin{aligned} w_{k|0} = q_k 2^{-\delta_{0k}\gamma} 2^{\frac{-\gamma_0}{\bar{p}}} \quad \forall k \in \{0,1\}, \\ w_{k|1} = q_k 2^{-\delta_{1k}\gamma} 2^{\frac{-\gamma_1}{p}} \quad \forall k \in \{0,1\}. \end{aligned}$$

Letting $\alpha \triangleq 2^{-\mu}$ and noticing that $w_{0|j} + w_{1|j} = 1$ $\forall j \in \{0,1\}$, we get

$$\begin{aligned} w_{0|0} = \frac{q_0}{q_0 + q_1\alpha}, \quad w_{0|1} = \frac{q_0\alpha}{q_0\alpha + q_1}, \\ w_{1|0} = \frac{q_1\alpha}{q_0 + q_1\alpha}, \quad w_{1|1} = \frac{q_1}{q_0\alpha + q_1}. \end{aligned}$$

Putting this into the constraints

$$\begin{cases} \bar{p}w_{0|0} + pw_{0|1} + 2\bar{p}w_{1|0} = D \\ q_0 = \bar{p}w_{0|0} + pw_{0|1} \\ q_1 = \bar{p}w_{1|0} + pw_{1|1} \end{cases}$$

[10] Here we use some abuse of notation and still write the optimizing values in their old forms without a $\star$ notation.

we have a set of 3 equations involving 3 variables α, q_0, q_1. Solving this gives us

$$\alpha = \frac{D+p-1}{2-(D+p)},$$
$$q_0 = \frac{2(1-p)-D}{3-2(D+p)},$$
$$q_1 = \frac{1-D}{3-2(D+p)}.$$

Therefore, we can obtain the optimizing $w_{k|j}$ and have

$$\begin{aligned} R &= H(p) - H(\frac{1}{1+\alpha}) \\ &= H(p) - H(D+p-1). \end{aligned}$$

Hence, in all cases $R = [H(p) - H(D+p-1)]^{+}$ and we conclude the proof. ■

Appendix C

Proof of Theorem 3

Proof: The objective here is to compute the RD function for a discrete source sequence x^N of i.n.d. source components x_i. First, with the notations $p_{i,j} \triangleq \Pr(X_i = j)$ and $q_{i,j} \triangleq \Pr(\hat{X}_i = j)$ for $j \in \{0,1\}$ and $i \in \{1,2,\dots N\}$, Lemma 6 gives us the rate-distortion components

$$R_i(D_i) = [H(p_i) - H(D_i + p_{i,1} - 1)]^{+}$$

along with the test-channel input-probability distributions

$$q_{i,0} = \frac{2(1-p_{i,1})-D_i}{3-2(p_{i,1}+D_i)} \quad \text{and} \quad q_{i,1} = \frac{1-D_i}{3-2(p_{i,1}+D_i)}$$

for each index i of the codeword. The overall rate-distortion function is given by

$$\begin{aligned} R(D) &= \min_{\sum_{i=1}^{N} D_i = D} R_i(D_i) \\ &= \min_{\sum_{i=1}^{N} D_i = D} \sum_{i=1}^{N} [H(p_i) - H(D_i + p_{i,1} - 1)]^{+} \end{aligned}$$

which is a convex optimization problem.

Using Lagrange multipliers, we form the functional

$$J(D) = \sum_{i=1}^{N} (H(p_{i,1}) - H(D_i + p_{i,1} - 1)) + \gamma \left(\sum_{i=1}^{N} D_i - D \right)$$

and compute the derivatives

$$\frac{\partial J}{\partial D_i} = \log(\frac{D_i + p_{i,1} - 1}{2 - D_i - p_{i,1}}) + \gamma.$$

The Kuhn-Tucker condition (see the restated version in [29], page 86) then tells us that there is γ such that

$$\frac{\partial J}{\partial D_i}\begin{cases} = 0 & \text{if}\, R_i(D_i) > 0 \\ \le 0 & \text{if}\, R_i(D_i) = 0 \end{cases}$$

which is equivalent to

$$\frac{D_i + p_{i,1} - 1}{2 - D_i - p_{i,1}}\begin{cases} = 2^{-\gamma} & \text{if}\, H(p_{i,1}) - H(D_i + p_{i,1} - 1) > 0 \\ \le 2^{-\gamma} & \text{if}\, H(p_{i,1}) - H(D_i + p_{i,1} - 1) \le 0 \end{cases}.$$

With the notations $\tilde{D}_i \triangleq D_i + p_{i,1} - 1$ and $\lambda \triangleq \frac{2^{-\gamma}}{1+2^{-\gamma}}$, it is equivalent to

$$\tilde{D}_i\begin{cases} = \lambda & \text{if}\, \tilde{D}_i < \min\{p_{i,1}, 1 - p_{i,1}\} \\ \le \lambda & \text{otherwise} \end{cases}.$$

Finally, it becomes

$$\tilde{D}_i = \begin{cases} \lambda & \text{if}\, \lambda < \min\{p_{i,1}, 1 - p_{i,1}\} \\ \min\{p_{i,1}, 1 - p_{i,1}\} & \text{otherwise} \end{cases}$$

where

$$\begin{aligned}\sum_{i=1}^{N} \tilde{D}_i &= \sum_{i=1}^{N} (D_i + p_{i,1} - 1) \\ &= D + \sum_{i=1}^{N} p_{i,1} - N\end{aligned}$$

and we conclude the proof. ■

Appendix D
Analysis of RDE Computation

Consider a binary single source X with $\Pr(X = 1) = p$ and $\Pr(X = 0) = 1 - p \triangleq \bar{p}$. According to [21], for any admissible (R, D) pair we can find two parameters $s \ge 0$ and $t \le 0$ so that $F(R, D)$ can be parametrically evaluated as

$$\begin{aligned} F(R, D) &= sR - stD + \max_{q_1} \left(-\log f(q_1)\right) \\ &= sR - stD - \log \min_{q_1} f(q_1) \end{aligned}$$

where

$$f(q_1) = \bar{p}\left(\sum_k q_k 2^{t\delta_{0k}}\right)^{-s} + p\left(\sum_k q_k 2^{t\delta_{1k}}\right)^{-s}$$

and R, D are given in terms of optimizing $\underline{q}^\star$.

For the distortion measure in (2) and with $q_0 = 1 - q_1$, we have

$$f(q_1) = \bar{p}\left((1-q_1)2^t + q_1 2^{2t}\right)^{-s} + p\left((1-q_1)2^t + q_1\right)^{-s}$$

which is a convex function in q_1. Taking the derivative $\frac{\partial f}{\partial q_1} = 0$ gives us

$$q_1^\star = \frac{1+2^t}{1-2^t}\left(\frac{1}{1+2^t} - \frac{\bar{p}^{\frac{1}{s+1}}}{2^{\frac{st}{s+1}}p^{\frac{1}{s+1}} + \bar{p}^{\frac{1}{s+1}}}\right) \triangleq \beta.$$

In order to minimize $f(q_1)$ over $q_1 \in [0,1]$, we consider three following cases where the optimal $q_1^\star$ is either on the boundary or at a point with zero gradient.

• Case 1: $0 \leq p \leq \frac{2^t}{1+2^t}$ then $\beta \leq 0$. Since f convex, it is non-decreasing in the interval $[\beta, \infty)$ and therefore in the interval $[0,1]$. Thus, the optimal $q_1^\star = 0$ and we can also compute

$$D = 1; \quad R = 0; \quad F = 0 = D_{KL}(p||p).$$

• Case 2: $1 \geq p \geq \frac{1}{1+2^{t(2s+1)}}$ then $\beta \geq 1$. Since f convex, it is non-increasing in the interval $(-\infty, \beta]$ and therefore in the interval $[0,1]$. Thus, the optimal $q_1^\star = 1$ and we get

$$D = \frac{2\bar{p}}{p2^{2ts} + \bar{p}}; \quad R = 0; \quad F = D_{KL}(u||p)$$

where in this case $u = 1 - \frac{D}{2}$. We can further see that $D \in [2(1-p), 1]$ and $u \in [1-D, p]$.

• Case 3: $\frac{2^t}{1+2^t} < p < \frac{1}{1+2^{t(2s+1)}}$ then $\beta \in (0,1)$. In this case, the optimal $q_1^\star = \beta$. We can find $w_{k|j}^\star = \frac{q_k^\star 2^{t\delta_{jk}}}{\sum_k q_k^\star 2^{t\delta_{jk}}}$ according to [21] and then obtain

$$\begin{aligned} D &= \frac{2^t}{1+2^t} + 1 - u, \\ R &= H(u) - H(u+D-1), \\ F &= D_{KL}(u||p) \end{aligned}$$

where

$$u = \frac{2^{\frac{st}{s+1}}p^{\frac{1}{s+1}}}{2^{\frac{st}{s+1}}p^{\frac{1}{s+1}} + \bar{p}^{\frac{1}{s+1}}}.$$

With this notation of u, we can express

$$q_1^\star = \frac{1-D}{3-2(u+D)} \quad \text{and} \quad q_0^\star = \frac{2(1-u)-D}{3-2(u+D)}.$$

We can see that $D \in (1-p, 1)$. It can also be verified that, in this case, by varying s and t, u spans $(1-D, 1-\frac{D}{2})$ and R spans $(0, H(1-D))$.

ACKNOWLEDGEMENT

The authors would like to acknowledge the support of Seagate through the NSF GOALI Program and thank Fatih Erden and Xinmiao Zhang for valuable discussions on this topic. The authors are also grateful to the associate editor and anonymous reviewers for comments that improved the quality of the paper.

REFERENCES

[1] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Indust. Math.*, vol. 8, no. 2, pp. 300–304, 1960.

[2] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and Algebraic-Geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

[3] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.

[4] G. D. Forney, Jr., "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. 12, no. 2, pp. 125–131, April 1966.

[5] S.-W. Lee and B. V. K. V. Kumar, "Soft-decision decoding of Reed-Solomon codes using successive error-and-erasure decoding," in *Proc. IEEE Global Telecom. Conf.*, New Orleans, LA, Nov. 2008, pp. 1–5.

[6] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, vol. 18, no. 1, pp. 170–182, Jan. 1972.

[7] H. Tang, Y. Liu, M. Fossorier, and S. Lin, "On combining Chase-2 and GMD decoding algorithms for nonbinary block codes," *IEEE Commun. Letters*, vol. 5, no. 5, pp. 209–211, May 2001.

[8] H. Tokushige, I. Hisadomi, and T. Kasami, "Selection of test patterns in an iterative erasure and error decoding algorithm for non-binary block codes," *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 11, pp. 3355–3359, Nov. 2006.

[9] J. Bellorado and A. Kavčić, "Low-complexity soft-decoding algorithms for Reed-Solomon codes - part I: An algebraic soft-in hard-out Chase decoder," *IEEE Trans. Inform. Theory*, vol. 56, no. 3, pp. 945–959, 2010.

[10] H. Xia and J. R. Cruz, "Reliability-based forward recursive algorithms for algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 55, no. 7, pp. 1273–1278, July 2007.

[11] H. Xia, H. Wang, and J. R. Cruz, "A Chase-GMD algorithm for soft-decision decoding of Reed-Solomon codes on perpendicular channels," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 1977–1981.

[12] J. Jiang and K. R. Narayanan, "Iterative soft-input-soft-output decoding of Reed-Solomon codes by adapting the parity-check matrix," *IEEE Trans. Inform. Theory*, vol. 52, no. 8, pp. 3746–3756, 2006.

[13] M. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on order statistics," *IEEE Trans. Inform. Theory*, vol. 41, no. 5, pp. 1379–1396, 1995.

[14] F. Parvaresh and A. Vardy, "Multiplicity assignments for algebraic soft-decoding of Reed-Solomon codes," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, July 2003, p. 205.

[15] M. El-Khamy and R. J. McEliece, "Interpolation multiplicity assignment algorithms for algebraic soft-decision decoding of Reed-Solomon codes," *AMS-DIMACS volume on Algebraic Coding Theory and Information Theory*, vol. 68, pp. 99–120, 2005.

[16] N. Ratnakar and R. Koetter, "Exponential error bounds for algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 11, pp. 3899–3917, 2005.

[17] H. Das and A. Vardy, "Multiplicity assignments for algebraic soft-decoding of Reed-Solomon codes using the method of types," in *Proc. IEEE Int. Symp. Information Theory*, Seoul, Korea, June 2009, pp. 1248–1252.

[18] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1983, iSBN 0-13-283796-X.

[19] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge University Press, 2003, iSBN-10 0521553741.

[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, 1991.

[21] R. E. Blahut, "Hypothesis testing and information theory," *IEEE Trans. Inform. Theory*, vol. 20, no. 4, pp. 405–417, July 1974.

[22] K. Marton, "Error exponent for source coding with a fidelity criterion," *IEEE Trans. Inform. Theory*, vol. 20, no. 2, pp. 197–199, March 1974.

[23] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Channels*. Akademiai Kiado, Budapest, Hungary, 1981.

[24] R. E. Blahut, *Principles and practice of information theory*. Addison-Wesley, 1987, iSBN-0201107090.

[25] ——, "Computation of channel capacity and rate distortion functions," *IEEE Trans. Inform. Theory*, vol. 18, no. 4, pp. 460–473, July 1972.

[26] T. Berger, *Rate Distortion Theory*. Englewood Cliffs, N.J., USA: Prentice-Hall, Inc., 1971, iSBN 13-753103-6.

[27] I. Csiszar, "On the computation of rate-distortion functions," *IEEE Trans. Inform. Theory*, vol. 20, no. 1, pp. 122–124, Jan. 1974.

[28] S. Arimoto, "Computation of random coding exponent functions," *IEEE Trans. Inform. Theory*, vol. 22, no. 6, pp. 665–671, Nov. 1976.

[29] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.

[30] G. Matz and P. Duhamel, "Information geometric formulation and interpretation of accelerated Blahut-Arimoto-type algorithms," in *Proc. IEEE Inform. Theory Workshop*, San Antonio, TX, Oct. 2004, pp. 66–70.

[31] R. J. McEliece, "The Guruswami-Sudan decoding algorithm for Reed-Solomon codes," *JPL Interplanetary Network Progress Report*, pp. 42–153, May 2003.

[32] W. J. Gross, F. R. Kschischang, R. Koetter, and P. G. Gulak, "Applications of algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1224–1234, 2006.

[33] X. Zhang, "Reduced complexity interpolation architecture for soft-decision Reed-Solomon decoding," *IEEE Trans. VLSI Syst.*, vol. 14, no. 10, pp. 1156–1161, 2006.

[34] J. Ma, A. Vardy, and Z. Wang, "Low-latency factorization architecture for algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. VLSI Syst.*, vol. 15, no. 11, pp. 1225–1238, 2007.

[35] J. Jiang and K. R. Narayanan, "Algebraic soft-decision decoding of Reed-Solomon codes using bit-level soft information," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3907–3928, Sept. 2008.

[36] H. Tokushige, T. Koumoto, M. Fossorier, and T. Kasami, "Selection method of test patterns in soft-decision iterative bounded distance decoding algorithms," *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, no. 10, pp. 2445–2451, Oct. 2003.