

# On Asymptotic Strategies for GMD Decoding with Arbitrary Error-Erasure Tradeoff

Joschi Brauchle, Vladimir Sidorenko

► **To cite this version:**

Joschi Brauchle, Vladimir Sidorenko. On Asymptotic Strategies for GMD Decoding with Arbitrary Error-Erasure Tradeoff. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Apr 2015, Paris, France. 2016, Proceedings of the 9th International Workshop on Coding and Cryptography 2015 WCC2015. <hal-01276219>

**HAL Id: hal-01276219**

**<https://hal.inria.fr/hal-01276219>**

Submitted on 19 Feb 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On Asymptotic Strategies for GMD Decoding with Arbitrary Error-Erasure Tradeoff

Joschi Brauchle\* and Vladimir Sidorenko\*\*

Institute for Communications Engineering,  
Technische Universität München  
Arcisstrasse 21, 80290 Munich, Germany  
{joschi.brauchle,vladimir.sidorenko}@tum.de

**Abstract.** Consider a block code  $\mathcal{C}$  of length  $n$  with Hamming distance  $d$ . Assume we have a decoder  $\Phi$ , which corrects  $e$  errors and  $t$  erasures, as soon as  $\lambda e + t \leq d - 1$ , where the real number  $1 < \lambda \leq 2$  is the *error-erasure tradeoff* of the decoder  $\Phi$ . In the classical case of bounded minimum distance decoder we have  $\lambda = 2$ , while smaller values of  $\lambda$  arise in decoding, e.g., interleaved or folded Reed–Solomon codes, as well as in algebraic decoding algorithms like Sudan or Guruswami–Sudan. Given a word  $\mathbf{r}$  with reliabilities of symbols, the goal of *generalized minimum distance (GMD)* decoding is to find a nearest codeword  $\mathbf{c} \in \mathcal{C}$  in *generalized Hamming metric*, defined by these reliabilities. We use multi-trial GMD Forney’s decoder, which at every trial applies  $\Phi$  to decode  $\mathbf{r}$ , where some low reliable symbols are erased. We investigate different erasing *strategies* based on either erasing a *fraction* of the received symbols or erasing all symbols whose reliability values are below a certain *threshold*. The erasing strategy may be either *static or adaptive*, where adaptive means that the erasing parameters are a function of the reliabilities. For every strategy we propose an optimal set of parameters and evaluate the error-correction radius of *m-trial* GMD decoder defined by each strategy. We use an asymptotic approach, i.e., large  $n$ , which drastically simplifies the analysis and presentation of the results over existing literature.

## 1 Introduction

Generalized minimum distance (GMD) decoding was introduced by Forney [3] to use reliability of received symbols together with algebraic (or other hard) decoding algorithms for error correction. The main idea is to use a simple algebraic error-erasure decoder in a multi-trial manner. An algebraic decoder can correct  $\lambda$  times more erasures than errors, where the real number  $1 < \lambda \leq 2$  is called the error-erasure tradeoff of the decoder. For each trial, a certain number of low reliable symbols are erased. As a result, at some trial the decoder can correct more errors than before since the most unreliable symbols, which are most likely

---

\* J. Brauchle’s work was supported by an Alexander von Humboldt Professorship endowed by the German Federal Ministry of Education and Research.

\*\* V. Sidorenko is on leave from the Institute for Information Transmission Problems, Russian Academy of Sciences.

to be erroneous, are erased. GMD decoding can be applied for an arbitrary code for which an efficient error-erasure decoder is known. The complexity of GMD decoding is at most  $m$  times the complexity of the algebraic decoder. Thus, GMD decoding is a universal and simple method for soft decoding.

Many variations, extensions, and improvements to the GMD decoding principle have been proposed over the years for the classical case of error-erasure tradeoff  $\lambda = 2$ , i.e., with a bounded minimum distance decoder correcting up to  $(d-1)/2$  errors, where  $d$  is the code distance in Hamming metric. For example, Kovalev [5] and Weber and Abdel-Ghaffar [10] studied the effects of reducing the maximum number of decoding trials. Sidorenko et al. [8] introduced GMD decoding with a bounded distance decoder correcting up to  $(d-t-1)/\lambda$  errors, where  $t$  is the number of erasures, and error-erasure tradeoff  $1 < \lambda \leq 2$ . Values of  $\lambda \leq 2$  are of interest for decoding  $l$ -interleaved or  $l$ -folded Reed–Solomon codes [1, 6], for which  $\lambda = {}^{(l+1)}/l$ , as well as for some modern algebraic decoders like the Sudan and Guruswami–Sudan [4] algorithms.

In this paper, we investigate different erasing *strategies* based on either erasing a *fraction* (F) of the received symbols or erasing all symbols whose reliability values are below a certain *threshold* (T). The erasing strategy may be either *static* (S) or *adaptive* (A), where adaptive means that the erasing is a function of the reliabilities. All four combinations are considered: static strategies SF and ST in Sections 3 and 4 as well as adaptive strategies AF and AT in Sections 5 and 6.

Like in [9], we use an asymptotic approach, i.e., the case of large code length  $n$ , which drastically simplifies the analysis and presentation of the results over existing literature, see [2, 5, 7–10] and references inside. In contrast to [9] where single-trial GMD decoding was considered, the more general case of an  $m$ -trial decoder is presented here, where  $m = 1, 2, \dots$  is the number of decoding trials. For every erasing strategy we propose an optimal set of parameters and evaluate the error-correction radius of an  $m$ -trial GMD decoder with optimal parameters. An adaptive multi-trial threshold erasing strategy has not been considered before and is a new result. Known multi-trial erasing strategies as well as the newly proposed one are evaluated in this context.

## 2 Definitions and Problem Statement

Assume a codeword  $\mathbf{c} = (c_1, \dots, c_n)$  from a code  $\mathcal{C}$  of length  $n$  and Hamming distance  $d$  over alphabet  $\mathcal{Q}$  is transmitted over a channel which may distort the transmitted symbols. Let  $\mathbf{z} = (z_1, \dots, z_n)$  be the channel output, where  $z_i$  does not necessarily belong to the code alphabet  $\mathcal{Q}$ . A detector delivers a symbol  $r_i \in \mathcal{Q}$ ,  $i = 1, \dots, n$ , which denotes the detector’s estimate of  $c_i$  based on  $z_i$ , and a reliability value  $\alpha_i \in [0, 1]$ , which represents the detector’s confidence in its estimate. The decoder input consists of the received vector  $\mathbf{r} = (r_1, \dots, r_n)$  and the associated reliability vector  $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ . The lower  $\alpha_i$ , the less reliable is the symbol  $r_i$ , with  $\alpha_i = 0$  corresponding to “fully unreliable”. Throughout the rest of the paper we will assume without loss of generality that the ordering of the received symbols is such that  $\alpha_i \leq \alpha_{i+1}$  for  $i = 1, \dots, n - 1$ .

The *generalized Hamming distance* between a received word  $\mathbf{r}$  with reliability vector  $\boldsymbol{\alpha}$  and a vector  $\mathbf{v} = (v_1, \dots, v_n) \in \mathcal{Q}^n$  is defined as

$$d_{\boldsymbol{\alpha}}(\mathbf{v}, \mathbf{r}) = \sum_{i:v_i=r_i} \frac{1-\alpha_i}{2} + \sum_{i:v_i \neq r_i} \frac{1+\alpha_i}{2} = \sum_{i=1}^n \frac{1-\alpha_i}{2} + \sum_{i:v_i \neq r_i} \alpha_i. \quad (1)$$

Note that this measure does not satisfy all requirements of a metric, since  $\mathbf{v} = \mathbf{r}$  does not necessarily imply  $d_{\boldsymbol{\alpha}}(\mathbf{v}, \mathbf{r}) = 0$ . In case  $\alpha_i = 1$  for all  $i$ , the generalized distance  $d_{\boldsymbol{\alpha}}(\mathbf{v}, \mathbf{r})$  reduces to the Hamming distance  $d_{\text{H}}(\mathbf{v}, \mathbf{r})$  between  $\mathbf{v}$  and  $\mathbf{r}$ . Decoding according to generalized distance is equivalent to maximum-likelihood decoding for some channels. It is also used in concatenated codes.

Let the *error-correction radius (ECR)* of a code  $\mathcal{C}$  be the infimum of all  $r \in \mathbb{R}$  for which there exist vectors  $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ ,  $\mathbf{r} \in \mathcal{Q}^n$ , and  $\boldsymbol{\alpha} \in [0, 1]^n$  such that  $\mathbf{c}' \neq \mathbf{c}$  and  $d_{\boldsymbol{\alpha}}(\mathbf{c}', \mathbf{r}) \leq d_{\boldsymbol{\alpha}}(\mathbf{c}, \mathbf{r}) = r$ . It is well known [3, 10], that the ECR equals  $d/2$ .

We use a bounded distance error-erasure decoder  $\Phi$  for the code  $\mathcal{C}$ , which is assumed to correct  $e$  errors and  $t$  erasures if and only if

$$\lambda e + t \leq d - 1, \quad (2)$$

where  $\lambda$  denotes the error-erasure tradeoff from the interval (1, 2]. For  $\lambda < 2$ , the decoder may fail, however the failure probability approaches zero (and will be neglected later) as the alphabet size  $|\mathcal{Q}|$  increases.

The *m-trial GMD decoder* works as follows. In trial  $j$ , where  $j = 1, \dots, m$ , a set of  $t_j$  least reliable symbols in  $\mathbf{r}$  is erased according to a certain strategy, and the resulting vector is decoded using  $\Phi$ , which produces either a codeword estimate  $\hat{\mathbf{c}}_j$  or a decoding failure. Among the (at most)  $m$  estimates  $\hat{\mathbf{c}}_j$ , one minimizing  $d_{\boldsymbol{\alpha}}(\hat{\mathbf{c}}_j, \mathbf{r})$  is chosen as the final decoder output. In case all trials fail, there is no codeword estimate at the output. Thus, the GMD decoder is defined by the erasing vector  $\mathbf{t} = (t_1, t_2, \dots, t_m)$  and is denoted by  $\text{GMD}(\mathbf{t})$ .

The *error-correction radius achievable by the decoder* is defined as the infimum of all  $r \in \mathbb{R}$  for which there exist  $\mathbf{c} \in \mathcal{C}$ ,  $\mathbf{r} \in \mathcal{Q}^n$ , and  $\boldsymbol{\alpha} \in [0, 1]^n$  so that  $d_{\boldsymbol{\alpha}}(\mathbf{c}, \mathbf{r}) = r$  and decoding is unsuccessful, i.e., the decoder reports a failure or outputs a codeword  $\hat{\mathbf{c}} \neq \mathbf{c}$ . The *normalized error-correction radius (NECR) achievable by the decoder*, denoted by  $\rho$ , is this number divided by the code's ECR, which equals  $d/2$ . Hence,  $\rho$  satisfies  $0 \leq \rho \leq 1$  and may be considered as the fraction of the code's ECR achievable by the decoding strategy under consideration. To find the NECR for all decoding strategies the following Lemma 1 is used. Given a reliability vector  $\boldsymbol{\alpha} \in [0, 1]^n$  and erasing vector  $\mathbf{t}$ , let  $D_{\boldsymbol{\alpha}}(\mathbf{t})$  denote the smallest normalized generalized distance between codeword  $\mathbf{c}$  and received word  $\mathbf{r}$  among all pairs, where  $\mathbf{c}$  is not the output of the  $\text{GMD}(\mathbf{t})$ , i.e.,

$$D_{\boldsymbol{\alpha}}(\mathbf{t}) = \min_{\mathbf{c} \in \mathcal{C}, \mathbf{r} \in \mathcal{Q}^n: \text{GMD}(\mathbf{t}) \neq \mathbf{c}} \frac{2d_{\boldsymbol{\alpha}}(\mathbf{c}, \mathbf{r})}{d}.$$

**Lemma 1 (See [2]).** For any  $\boldsymbol{\alpha} \in [0, 1]^n$  and  $\mathbf{t} = (t_1, t_2, \dots, t_m)$ ,

$$D_{\boldsymbol{\alpha}}(\mathbf{t}) = \frac{1}{d} \left( n - \sum_{i=1}^n \alpha_i + 2 \sum_{i=1}^m \sum_{j=t_i+1}^{t_i+e(t_i)-e(t_{i+1})} \alpha_i \right), \quad (3)$$

where

$$e(t) = \left\lfloor \frac{(d-t-1)}{\lambda} \right\rfloor + 1, \quad (4)$$

denotes the error-correction radius of the decoder  $\Phi$  in presence of  $t$  erasures, with formally  $t_{m+1} = d$ , such that  $e(t_{m+1}) = 0$ .

## 2.1 Asymptotic Approach

Using Lemma 1 to evaluate the error-correction radii of erasing strategies like in previous publications leads to cumbersome expressions in which several subcases need to be distinguished. Here, we will restrict ourselves to asymptotic analysis, i.e., long codes and represent reliability information by a function  $h$  instead of a vector  $\alpha$ , yielding huge simplifications in the evaluation and final expressions.

We normalize the Hamming distance  $d$ , number of erasures  $t$  and errors  $e$  to the code length  $n$  by introducing  $\delta = d/n$ ,  $\tau = t/n$ , and  $\varepsilon = e/n$ , where  $0 < \delta \leq 1$ ,  $0 \leq \tau \leq 1$ , and  $0 \leq \varepsilon \leq 1$ . The error-correction radius of decoder  $\Phi$  from (4) is also normalized to  $n$  and in the presence of  $\tau n$  erasures simplifies to

$$\varepsilon(\tau) = \frac{\delta - \tau}{\lambda}. \quad (5)$$

Let  $h$  denote a function on the interval  $(0, 1]$  taking values from the interval  $[0, 1]$ . We assume  $h$  to be non-decreasing to comply with the previous assumption  $\alpha_i \leq \alpha_{i+1}$ . For any erasing vector  $\tau = (\tau_1, \dots, \tau_m)$ , where  $0 \leq \tau_1 < \tau_2 < \dots < \tau_m \leq \delta$ , and such function  $h$ , define

$$\Delta_h(\tau) = \frac{1}{\delta} \left( 1 - \int_0^1 h(\phi) d\phi + 2 \sum_{i=1}^m \int_{\tau_i}^{\tau_i + \varepsilon(\tau_i) - \varepsilon(\tau_{i+1})} h(\phi) d\phi \right), \quad (6)$$

where  $\varepsilon(\tau_i) - \varepsilon(\tau_{i+1}) = (\tau_{i+1} - \tau_i)/\lambda$  and formally  $\tau_{m+1} = \delta$ , such that  $\varepsilon(\tau_{m+1}) = 0$ .

**Lemma 2.** *When taking  $h(\phi) = \alpha_{\lceil \phi n \rceil}$  for  $0 < \phi \leq 1$ , it holds that*

$$\lim_{n \rightarrow \infty} D_{\alpha}(\tau n) = \Delta_h(\tau).$$

Lemma 2 provides a tool to perform asymptotic analysis of erasing strategies based on the reliability function  $h$  which is easier to handle than the reliability vector  $\alpha$ . In our analysis we use special *step reliability functions* defined by two vectors  $\mu = (\mu_1, \dots, \mu_k)$  and  $\nu = (\nu_1, \dots, \nu_k)$ , and denoted by

$$s_{\mu, \nu}(\phi) = \nu_i \quad \text{for } \mu_{i-1} \leq \phi < \mu_i, \quad i = 1, \dots, k+1, \quad (7)$$

where  $\mu_0 \triangleq 0 \leq \mu_1 \leq \dots \leq \mu_k \leq \mu_{k+1} \triangleq 1$  and  $\nu_0 \triangleq 0 \leq \nu_1 \leq \dots \leq \nu_k \leq \nu_{k+1} \triangleq 1$ . For the unit step function with  $k = 1$  and  $\nu_1 = 0$ , we write  $s_{\mu_1}(\phi) \triangleq s_{(\mu_1), (0)}(\phi)$ .

### 3 Static Fraction Erasing

When fixing the erasing vector  $\boldsymbol{\tau}$  prior to reception of a certain reliability function  $h$ , an NECR of  $\rho_{\text{SF}}(\boldsymbol{\tau}) = \inf_h \Delta_h(\boldsymbol{\tau})$  is achievable. The parameter  $\boldsymbol{\tau}$  can be chosen to maximize the achievable NECR. Hence, the maximum achievable NECR for the static fraction (SF) erasing strategy is given by

$$\rho_{\text{SF}} = \max_{\boldsymbol{\tau}} \inf_h \Delta_h(\boldsymbol{\tau}). \quad (8)$$

Let us consider the following system of difference equations to find the optimal erasing vector  $\boldsymbol{\tau}$

$$\tau_{i+1} = \lambda\tau_i - (\lambda - 1)\tau_{i-1}, \quad i = 1, \dots, m, \quad (9)$$

with boundary conditions  $\tau_0 = \frac{\tau_1}{1-\lambda}$  and  $\tau_{m+1} = \delta$ , which is solved by

$$\tau_i = \delta \frac{\lambda \sum_{k=0}^{i-1} (\lambda - 1)^k - 1}{\lambda \sum_{k=0}^m (\lambda - 1)^k - 1} = \begin{cases} \delta \frac{2^i - 1}{2^{m+1}} & \text{for } \lambda = 2 \\ \delta \frac{\lambda^{i-1} - 1}{\lambda(\lambda - 1)^{m-2}} & \text{for } \lambda < 2. \end{cases} \quad (10)$$

Note that the solutions are qualitatively different: for the classical case of  $\lambda = 2$ ,  $\tau_i$  is a linear function of  $i$ , whereas for  $\lambda < 2$  it is an exponential function!

**Lemma 3.** *For static fraction erasing,*

$$\rho_{\text{SF}} = \frac{1}{\delta} \frac{\delta + (\lambda - 1)\tau_m}{\lambda} = \frac{1}{\delta} \frac{2\delta - \tau_1}{\lambda} \quad (11)$$

is achievable by choosing  $\boldsymbol{\tau} = (\tau_1, \tau_2, \dots, \tau_m)$  and  $\tau_i$  as in (10).

*Proof.* First, let us find a lower bound on  $\rho_{\text{SF}}$ . For any  $h$  we have

$$\begin{aligned} \Delta_h(\boldsymbol{\tau}) &= \frac{1}{\delta} \left( 1 - \sum_{i=1}^m \left[ \int_{\frac{(\lambda-1)\tau_{i-1} + \tau_i}{\lambda}}^{\tau_i} h(\phi) d\phi - \int_{\tau_i}^{\frac{(\lambda-1)\tau_i + \tau_{i+1}}{\lambda}} h(\phi) d\phi \right] - \int_{\frac{\delta + (\lambda-1)\tau_m}{\lambda}}^1 h(\phi) d\phi \right) \\ &\stackrel{(a)}{\geq} \frac{1}{\delta} \left( 1 - \sum_{i=1}^m h(\tau_i) \left[ \frac{\lambda\tau_i - (\lambda-1)\tau_{i-1} - \tau_{i+1}}{\lambda} \right] - \left[ 1 - \frac{\delta + (\lambda-1)\tau_m}{\lambda} \right] \right) \\ &\stackrel{(b)}{\geq} \frac{1}{\delta} \frac{\delta + (\lambda-1)\tau_m}{\lambda}, \end{aligned}$$

where the inequality (a) results from  $h$  being non-decreasing and (b) from the difference equations (9).

To get an upper bound on  $\rho_{\text{SF}}$  we show that for every  $\boldsymbol{\tau}' = (\tau'_1, \tau'_2, \dots, \tau'_m)$  where we formally assign  $\tau'_0(1-\lambda) = \tau'_1$ , and  $\tau'_{m+1} = \delta$ , there exists a (step) reliability function  $h$  such that  $\Delta_h(\boldsymbol{\tau}') \leq \rho_{\text{SF}}$ . Let  $j = \max_i \{i : \tau'_i \leq \tau_i\}, 0 \in$

$\{0, 1, \dots, m\}$  and  $h_j(\phi) = s_{(\tau'_{j+1} + (\lambda-1)\tau'_j)/\lambda}(\phi)$ . We have

$$\begin{aligned}
\Delta_{h_j}(\boldsymbol{\tau}') &= \frac{1}{\delta} \left( 1 - \int_{\frac{\tau'_{j+1} + (\lambda-1)\tau'_j}{\lambda}}^1 h_j(\phi) d\phi + 2 \sum_{i=j+1}^m \int_{\tau'_i}^{\frac{\tau'_{i+1} + (\lambda-1)\tau'_i}{\lambda}} h_j(\phi) d\phi \right) \\
&= \frac{1}{\delta} \left( 1 - \left[ 1 - \frac{\tau'_{j+1} + (\lambda-1)\tau'_j}{\lambda} \right] + 2 \sum_{i=j+1}^m \frac{\tau'_{i+1} - \tau'_i}{\lambda} \right) \\
&= \frac{1}{\delta} \left( \frac{\tau'_{j+1} + (\lambda-1)\tau'_j}{\lambda} + 2 \frac{\delta - \tau'_{j+1}}{\lambda} \right) = \frac{1}{\delta} \frac{2\delta + (\lambda-1)\tau'_j - \tau'_{j+1}}{\lambda} \\
&\stackrel{(a)}{\leq} \frac{1}{\delta} \frac{2\delta + (\lambda-1)\tau_j - \tau_{j+1}}{\lambda} \stackrel{(b)}{=} \frac{1}{\delta} \frac{\delta + (\lambda-1)\tau_m}{\lambda},
\end{aligned}$$

where we define  $\sum_a^b \phi = 0$  if  $a > b$ . Inequality (a) follows from  $\tau'_{j+1} \geq \tau_{j+1}$ ,  $\tau'_j \leq \tau_j$ , due to the definition of  $j$ , and equality (b) results from the difference equations (9) and boundary condition  $\tau'_{m+1} = \delta$ .  $\square$

**Theorem 1.** *For static fraction erasing, the maximum achievable NECR*

$$\rho_{SF} = \frac{2 \sum_{k=0}^{m-1} (\lambda-1)^k}{\lambda \sum_{k=0}^{m-1} (\lambda-1)^k + 1} = \begin{cases} \frac{2m}{2m+1} & \text{for } \lambda = 2 \\ 2 \frac{(\lambda-1)^m - 1}{\lambda(\lambda-1)^m - 2} & \text{for } \lambda < 2 \end{cases}$$

is achievable by choosing  $\boldsymbol{\tau} = (\tau_1, \tau_2, \dots, \tau_m)$  given by (10).

*Proof.* By combining Lemma 3 and (10) the theorem follows.  $\square$

## 4 Static Threshold Erasing

In this section, the erasing strategy is based on erasing symbols with reliability values below a certain threshold, which is fixed prior to reception. For a static threshold (ST) erasing parameter  $\boldsymbol{\theta} = (\theta_1, \theta_2, \dots, \theta_m)$ , where  $0 \leq \theta_1 \leq \theta_2 \leq \dots \leq \theta_m \leq 1$ , and reliability function  $h$ , let

$$\tau_h(\theta_i) = \min\{\delta, \max\{0, \sup\{0 < \phi \leq 1 : h(\phi) < \theta_i\}\}\} \quad (12)$$

denote the fraction of received symbols, at most  $\delta$ , to be erased due to reliability values below threshold  $\theta_i$ , if any, or zero otherwise. We also define the vector  $\boldsymbol{\tau}_h(\boldsymbol{\theta}) = (\tau_h(\theta_1), \tau_h(\theta_2), \dots, \tau_h(\theta_m))$ , where  $0 \leq \tau_h(\theta_1) \leq \tau_h(\theta_2) \leq \dots \leq \tau_h(\theta_m) \leq 1$  as  $h$  is non-decreasing, and the function

$$\Gamma_h(\boldsymbol{\theta}) = \Delta_h(\boldsymbol{\tau}_h(\boldsymbol{\theta})) = \Delta_h(\tau_h(\theta_1), \tau_h(\theta_2), \dots, \tau_h(\theta_m)). \quad (13)$$

For this erasing strategy a NECR of  $\rho_{ST}(\boldsymbol{\theta}) = \inf_h \Gamma_h(\boldsymbol{\theta})$  is achievable, where the parameter  $\boldsymbol{\theta}$  can be chosen to maximize this value. Hence, the maximum achievable NECR for the static threshold erasing strategy is given by

$$\rho_{ST} = \max_{\boldsymbol{\theta}} \inf_h \Gamma_h(\boldsymbol{\theta}). \quad (14)$$

To derive an expression for  $\rho_{ST}$ , let us consider the following system of difference equations

$$\theta_{i-1} = \lambda\theta_i - (\lambda - 1)\theta_{i+1}, \quad i = 1, \dots, m, \quad (15)$$

with boundary conditions  $\theta_0 = -\theta_1$  and  $\theta_{m+1} = 1$ . The system is solved by

$$\theta_i = \frac{(\lambda - 1)^m}{(\lambda - 1)^{i-1}} \frac{\lambda \sum_{k=0}^{i-1} (\lambda - 1)^k - 1}{\lambda \sum_{k=0}^m (\lambda - 1)^k - 1} = \begin{cases} \frac{2i-1}{2m+1} & \text{for } \lambda = 2 \\ \frac{(\lambda-1)^m}{(\lambda-1)^{i-1}} \frac{\lambda(\lambda-1)^{i-1}-2}{\lambda(\lambda-1)^m-2} & \text{for } \lambda < 2 \end{cases} \quad (16)$$

for  $i = 1, \dots, m$ . The solutions are linear functions in  $i$  for the classical case of  $\lambda = 2$ , while there is an exponential relationship in  $i$  for  $\lambda < 2$ .

**Lemma 4.** *For static threshold erasing,*

$$\rho_{ST} = \frac{1 + \theta_m}{\lambda} = 1 - \theta_1 \quad (17)$$

is achievable by choosing  $\boldsymbol{\theta} = (\theta_1, \theta_2, \dots, \theta_m)$  and  $\theta_i$  as in (16).

*Proof.* We show (i) that for any  $h$  we have  $\Gamma_h(\boldsymbol{\theta}) \geq \rho_{ST}$  and (ii) that there exists a reliability function  $h$  such that for every choice of  $\boldsymbol{\theta}'$  it holds that  $\Gamma_h(\boldsymbol{\theta}') \leq \rho_{ST}$ . Hence, the statement of the theorem follows.

(i) For any  $h$  we have

$$\begin{aligned} \Gamma_h(\boldsymbol{\theta}) &= \Delta_h(\boldsymbol{\tau}_h(\boldsymbol{\theta})) \\ &= \frac{1}{\delta} \left( 1 - \sum_{i=1}^m \left[ \int_{\frac{(\lambda-1)\tau_h(\theta_{i-1})+\tau_h(\theta_i)}{\lambda}}^{\tau_h(\theta_i)} h(\phi) d\phi - \int_{\tau_h(\theta_i)}^{\frac{(\lambda-1)\tau_h(\theta_i)+\tau_h(\theta_{i+1})}{\lambda}} h(\phi) d\phi \right] - \int_{\frac{\delta+(\lambda-1)\tau_h(\theta_m)}{\lambda}}^1 h(\phi) d\phi \right) \\ &\stackrel{(a)}{\geq} \frac{1}{\delta} \left( \sum_{i=1}^m \theta_i \left[ \tau_h(\theta_i) - \frac{(\lambda-1)\tau_h(\theta_{i-1}) - \tau_h(\theta_{i+1})}{\lambda} \right] + \frac{\delta + (\lambda-1)\tau_h(\theta_m)}{\lambda} \right) \\ &\geq \frac{1}{\delta} \left( \delta \frac{1+\theta_m}{\lambda} - \sum_{i=1}^m \tau_h(\theta_i) \left[ \frac{\lambda\theta_i - (\lambda-1)\theta_{i+1} - \theta_{i-1}}{\lambda} \right] \right) \stackrel{(b)}{=} \frac{1+\theta_m}{\lambda} \stackrel{(c)}{=} 1 - \theta_1, \end{aligned}$$

where the inequality (a) results from  $h$  being non-decreasing and (b) and (c) from applying the difference equations (15).

(ii) It can be shown that for every choice of  $\boldsymbol{\theta}' = (\theta'_1, \theta'_2, \dots, \theta'_m)$  the reliability function  $h(\phi) = s_{(\delta/\lambda, \delta), (\theta'_j + \zeta, \theta'_{j+1} - \zeta)}(\phi)$  yields  $\Delta_h(\boldsymbol{\theta}') \leq \rho_{ST}$ , where we let  $j = \max_i \{i : \theta'_i \leq \theta_i\}$ ,  $0 \in \{0, 1, \dots, m\}$ , and  $\zeta > 0$  an arbitrarily small value.  $\square$

**Theorem 2.** *For static threshold erasing, the maximum achievable NECR is*

$$\rho_{ST} = \frac{2 \sum_{k=0}^{m-1} (\lambda - 1)^k}{\lambda \sum_{k=0}^{m-1} (\lambda - 1)^k + 1} = \begin{cases} \frac{2m}{2m+1} & \text{for } \lambda = 2 \\ 2 \frac{(\lambda-1)^m - 1}{\lambda(\lambda-1)^m - 2} & \text{for } \lambda < 2, \end{cases}$$

and  $\rho_{ST} = \rho_{SF}$ .

*Proof.* By combining Lemma 4 and (16) the statement follows.  $\square$

Note that the maximum achievable NECR of SF and ST strategies is identical, with an advantage for ST erasing that received symbols need not be ordered according to their reliabilities, but can be acted on immediately upon receipt.



## 5 Adaptive Fraction Erasing

In adaptive strategies, the erasing vector  $\boldsymbol{\tau}$  may be chosen to maximize  $\Delta_h(\boldsymbol{\tau})$  after the receipt of a certain reliability function  $h$ . Thus, the maximum achievable NECR for the adaptive fraction (AF) erasing strategy is given by

$$\rho_{\text{AF}} = \inf_h \max_{\boldsymbol{\tau}} \Delta_h(\boldsymbol{\tau}). \quad (18)$$

To derive an explicit expression for  $\rho_{\text{AF}}$ , let  $\boldsymbol{\mu} = (\mu_1, \dots, \mu_{2m-1})$  denote the solution of the following system of difference equations

$$\mu_{i+1} = \lambda\mu_i - (\lambda - 1)\mu_{i-1}, \quad i = 1, \dots, 2m - 1, \quad (19)$$

with boundary conditions  $\mu_0 = 0$  and  $\mu_{2m} = \delta$ , i.e.,

$$\mu_i = \delta \frac{\sum_{k=0}^{i-1} (\lambda - 1)^k}{\sum_{k=0}^{2m-1} (\lambda - 1)^k} = \begin{cases} \delta \frac{i}{2m} & \text{for } \lambda = 2 \\ \delta \frac{1 - (\lambda - 1)^i}{1 - (\lambda - 1)^{2m}} & \text{for } \lambda < 2. \end{cases} \quad (20)$$

Notice that the solutions are again qualitatively different: for the classical case of  $\lambda = 2$ ,  $\mu_i$  is a linear function of  $i$ , and for  $\lambda < 2$  it is an exponential function!

**Theorem 3.** *For adaptive fraction erasing, the maximum achievable NECR is*

$$\rho_{\text{AF}} = \frac{1}{\delta} \frac{\delta + (\lambda - 1)\mu_{2m-1}}{\lambda} = \frac{1}{\delta} \frac{2\delta - \mu_1}{\lambda} = \begin{cases} 1 - \frac{1}{4m} & \text{for } \lambda = 2 \\ 1 - \frac{(2-\lambda)(\lambda-1)^{2m}}{\lambda(1-(\lambda-1)^{2m})} & \text{for } \lambda < 2 \end{cases}$$

by choosing

$$\boldsymbol{\tau} = \begin{cases} \boldsymbol{\tau}^a & \text{if } \Delta_h(\boldsymbol{\tau}^a) \geq \Delta_h(\boldsymbol{\tau}^b), \\ \boldsymbol{\tau}^b & \text{otherwise,} \end{cases}$$

with  $\boldsymbol{\tau}^a = (\mu_0, \mu_2, \dots, \mu_{2m-2})$ ,  $\boldsymbol{\tau}^b = (\mu_1, \mu_3, \dots, \mu_{2m-1})$  and  $\mu_i$  as in (20).

*Proof.* We show (i) that for any  $h$  we have  $\Delta_h(\boldsymbol{\tau}) \geq \rho_{\text{AF}}$  for  $\boldsymbol{\tau} = \boldsymbol{\tau}^a$  or for  $\boldsymbol{\tau} = \boldsymbol{\tau}^b$  and (ii) that there exists a reliability function  $h$  such that for every choice of  $\boldsymbol{\tau}$  it holds that  $\Delta_h(\boldsymbol{\tau}) \leq \rho_{\text{AF}}$ . Hence, the statement of the theorem follows.

(i) For any  $h$  we have

$$\Delta_h(\boldsymbol{\tau}^a) + \Delta_h(\boldsymbol{\tau}^b) = \frac{2}{\delta} \left( 1 - \int_0^1 h(\phi) d\phi + \sum_{i=0}^{2m-1} \int_{\mu_i}^{\mu_i + \varepsilon(\mu_i) - \varepsilon(\mu_{i+2})} h(\phi) d\phi \right), \quad (21)$$

where we formally assign  $\mu_{2m+1} = \delta$ . Since the  $2m$  integration intervals cover the interval  $[0, \mu_{2m-1} + \varepsilon(\mu_{2m-1})]$  without gaps and intersections, we write

$$\Delta_h(\boldsymbol{\tau}^a) + \Delta_h(\boldsymbol{\tau}^b) = \frac{2}{\delta} \left( 1 - \int_{\mu_{2m-1} + \varepsilon(\mu_{2m-1})}^1 h(\phi) d\phi \right) \geq \frac{2}{\delta} \frac{\delta + (\lambda - 1)\mu_{2m-1}}{\lambda} = 2\rho_{\text{AF}}. \quad (22)$$

By Dirichlet's box principle, for any  $h$ , it holds that  $\Delta_h(\boldsymbol{\tau}) \geq \rho_{\text{AF}}$  for  $\boldsymbol{\tau} = \boldsymbol{\tau}^a$  or for  $\boldsymbol{\tau} = \boldsymbol{\tau}^b$ .

Statement (ii) can be shown for the function  $h(\phi) = s_{\boldsymbol{\mu}, \boldsymbol{\nu}}(\phi)$ , where components of vector  $\boldsymbol{\nu} = (\nu_1, \dots, \nu_{2m-1})$  satisfy

$$\nu_{i-1} = \lambda\nu_i - (\lambda - 1)\nu_{i+1}, \quad i = 1, \dots, 2m - 1, \quad (23)$$

with boundary conditions  $\nu_0 = 0$  and  $\nu_{2m} = 1$ .  $\square$

The maximum NECR of the adaptive fraction erasing strategy can be achieved using erasing vector  $\boldsymbol{\tau}$  by considering merely two options:  $\boldsymbol{\tau}^a$  and  $\boldsymbol{\tau}^b$ .

## 6 Adaptive Threshold Erasing

Upon receipt of a certain reliability function  $h$ , the threshold vector  $\boldsymbol{\theta}$  may be chosen such that  $\Gamma_h(\boldsymbol{\theta})$  is maximized. Hence, the maximum achievable NECR for the adaptive threshold (AT) erasing strategy is given by

$$\rho_{\text{AT}} = \inf_h \max_{\boldsymbol{\theta}} \Gamma_h(\boldsymbol{\theta}).$$

**Theorem 4.** *For adaptive threshold erasing a maximum NECR of*

$$\rho_{\text{AT}} = \rho_{\text{AF}}$$

*is achievable by choosing the vector of thresholds*

$$\boldsymbol{\theta} = \begin{cases} \boldsymbol{\theta}^a & \text{if } \Delta_h(\boldsymbol{\theta}^a) \geq \Delta_h(\boldsymbol{\theta}^b), \\ \boldsymbol{\theta}^b & \text{otherwise,} \end{cases}$$

where  $\boldsymbol{\theta}^a = (\nu_0, \nu_2, \dots, \nu_{2m-2})$ ,  $\boldsymbol{\theta}^b = (\nu_1, \nu_3, \dots, \nu_{2m-1})$ ,  $\nu_i$  as in (23) and  $\rho_{\text{AF}}$  as given by Theorem 3.

*Proof.* The upper bound  $\rho_{\text{AT}} \leq \rho_{\text{AF}}$  follows from Theorem 3 and the inequality

$$\inf_h \max_{\boldsymbol{\theta}} \Gamma_h(\boldsymbol{\theta}) = \inf_h \max_{\boldsymbol{\theta}} \Delta_h(\boldsymbol{\tau}_h(\boldsymbol{\theta})) \leq \inf_h \max_{\boldsymbol{\tau}} \Delta_h(\boldsymbol{\tau}) = \rho_{\text{AF}}.$$

To show that the lower bound  $\rho_{\text{AT}} \geq \rho_{\text{AF}}$  holds we let  $\mu_i = \tau_h(\nu_i)$  and consider

$$\begin{aligned} \Gamma_h(\boldsymbol{\theta}^a) + \Gamma_h(\boldsymbol{\theta}^b) &= \Delta_h(\boldsymbol{\tau}_h(\boldsymbol{\theta}^a)) + \Delta_h(\boldsymbol{\tau}_h(\boldsymbol{\theta}^b)) \\ &= \frac{2}{\delta} \left( 1 - \sum_{i=0}^{2m-1} \left[ \int_{\frac{(\lambda-1)\mu_{i-1} + \mu_i}{\lambda}}^{\mu_i} h(\phi) d\phi - \int_{\mu_i}^{\frac{(\lambda-1)\mu_i + \mu_{i+1}}{\lambda}} h(\phi) d\phi \right] - \int_{\frac{\delta + (\lambda-1)\mu_m}{\lambda}}^1 h(\phi) d\phi \right) \\ &\stackrel{(a)}{\geq} \frac{2}{\delta} \left( 1 - \sum_{i=0}^{2m-1} \nu_i \left[ \frac{\lambda\mu_i - (\lambda-1)\mu_{i-1} - \mu_{i+1}}{\lambda} \right] - \left[ 1 - \frac{\delta + (\lambda-1)\mu_m}{\lambda} \right] \right) \\ &= \frac{2}{\delta} \left( \delta \frac{1 + \nu_{2m-1}}{\lambda} - \sum_{i=0}^{2m-1} \mu_i \left[ \frac{\lambda\nu_i - (\lambda-1)\nu_{i+1} - \nu_{i-1}}{\lambda} \right] \right) \\ &\stackrel{(b)}{\geq} 2 \frac{1 + \nu_{2m-1}}{\lambda} \stackrel{(c)}{=} 2\rho_{\text{AF}}, \end{aligned}$$

where the inequality (a) results from  $h$  being non-decreasing and (b) and (c) from the difference equations (23). By Dirichlet's box principle,  $\Gamma_h(\boldsymbol{\theta}) \geq \rho_{\text{AF}}$  for any  $h$  and  $\boldsymbol{\theta} = \boldsymbol{\theta}^a$  or  $\boldsymbol{\theta} = \boldsymbol{\theta}^b$ , and thus  $\rho_{\text{AT}} \geq \rho_{\text{AF}}$ , and the theorem follows.  $\square$

## 7 Conclusion

In this paper, we investigated fraction-based and threshold-based multi-trial erasing strategies for GMD decoding with arbitrary error-erasure tradeoff. Both strategies achieve the same normalized error-correction radius (NECR), while the static threshold erasing strategy has the advantageous property that ordering of received symbols is not required. For the same number  $m$  of trials, the NECR of the adaptive strategy is larger than the static one, and the NECR generally increases with decreasing error-erasure tradeoff  $\lambda$ . To achieve an NECR of  $1 - \xi$ , the adaptive strategy requires only half the number  $m(\xi)$  of trials in comparison to the static one, where  $m(\xi)$  is  $\mathcal{O}(\xi^{-1})$  for the classical case of  $\lambda = 2$  and only  $\mathcal{O}(\log(\xi^{-1}))$  for the case of  $\lambda < 2$ .

## References

1. Brauchle, J.: On the Error-Correcting Radius of Folded Reed–Solomon Code Designs. In: 4th Int. Castle Meeting on Coding Theory and Appl. pp. 1–8 (2014)
2. Chaaban, A., Sidorenko, V.R., Senger, C.: On multi-trial Forney–Kovalev decoding of concatenated codes. *Adv. Math. Commun.* 8(1), 1–20 (2014)
3. Forney, Jr., G.D.: Generalized minimum distance decoding. *IEEE Trans. Inf. Theory* 12(2), 125–131 (Apr 1966)
4. Guruswami, V., Sudan, M.: Improved decoding of Reed–Solomon and algebraic-geometry codes. *IEEE Trans. Inf. Theory* 45(6), 1757–1767 (Sep 1999)
5. Kovalev, S.: Two classes of minimum generalized distance decoding algorithms. *Probl. Inf. Transm.* 22, 186–192 (1986)
6. Schmidt, G., Sidorenko, V.R., Bossert, M.: Collaborative Decoding of Interleaved Reed–Solomon Codes and Concatenated Code Designs. *IEEE Trans. Inf. Theory* 55(7), 2991–3012 (Jul 2009)
7. Senger, C., Sidorenko, V.R., Bossert, M., Zyablov, V.V.: Multitrial decoding of concatenated codes using fixed thresholds. *Probl. Inf. Transm.* 46(2), 127–141 (Jul 2010)
8. Sidorenko, V.R., Chaaban, A., Senger, C., Bossert, M.: On Extended Forney–Kovalev GMD decoding. In: *Proc. IEEE Int. Symp. on Inform. Theory*. pp. 1393–1397 (Jul 2009)
9. Weber, J.H., Sidorenko, V.R., Senger, C., Abdel-Ghaffar, K.A.S.: Asymptotic single-trial strategies for GMD decoding with arbitrary error-erasure tradeoff. *Probl. Inf. Transm.* 48(4), 324–333 (Jan 2013)
10. Weber, J., Abdel-Ghaffar, K.: Reduced GMD decoding. *IEEE Trans. Inf. Theory* 49(4), 1013–1027 (Apr 2003)