

Single-trial adaptive decoding of concatenated codes

VLADIMIR SIDORENKO¹

vladimir.sidorenko@uni-ulm.de

CHRISTIAN SENGER²

christian.senger@uni-ulm.de

MARTIN BOSSERT

martin.bossert@uni-ulm.de

TAIT, Ulm University, Ulm, Germany

VICTOR ZYABLOV

zyablov@iitp.ru

IITP, Russian Academy of Sciences, Moscow, Russia

Abstract. In this paper decoding of a concatenated code is considered. We use a Bounded Minimum Distance (BMD) decoder for the inner code correcting up to $(d^i - 1)/2$ errors and a Bounded Distance (BD) decoder for the outer code, which corrects ε errors and τ erasures if $\lambda\varepsilon + \tau \leq d^o - 1$, where a real number $1 < \lambda \leq 2$ is the tradeoff rate between errors and erasures for this outer decoder. Here d^o and d^i are the minimum distances of the outer and the inner code, respectively. We consider a single-trial outer decoder, which extends Kovalev's approach [1] for the whole given range of λ . The error correcting radius of the suggested concatenated decoder is $\frac{d^i d^o}{2} \left(1 - \left(\frac{\lambda-1}{\lambda}\right)^2\right)$. When using an outer Reed–Solomon code over $\mathbb{F}_{q^{\ell m}}$ of length $n^o \leq q^m$ with the BD decoder suggested in [2], $\lambda = \frac{\ell+1}{\ell}$, and the error correcting radius $\frac{d^i d^o}{2} \left(1 - \frac{1}{(1-\ell)^2}\right)$ of the concatenated decoder quickly approaches $d^i d^o / 2$ with increasing ℓ .

1 Introduction

Concatenated codes were suggested and investigated by Forney in 1966 [3]. A simple concatenated coding scheme uses an outer block code $\mathcal{C}^o(n^o, k^o, d^o)$ over the finite field $\mathbb{F}_{q^{k^i}}$ and an inner block code $\mathcal{C}^i(n^i, k^i, d^i)$ over \mathbb{F}_q , where the upper indices o and i stand for the outer and the inner code, respectively. The information sequence composed of k^o q^{k^i} -ary symbols is first encoded using the outer code into a q^{k^i} -ary codeword $\mathbf{c}^o = (c_1^o, \dots, c_{n^o}^o)$. The inner code is then used to encode each symbol c_j^o , $j = 1, \dots, n^o$, into a q -ary column vector $\mathbf{c}^{i,T} = (c_1^i, \dots, c_{n^i}^i)^T$. This results in an $n^i \times n^o$ matrix C of q -ary symbols, which is a codeword of the concatenated code \mathcal{C} . The code matrix C is transmitted over a q -ary channel and may suffer from channel errors. Denote by R the received matrix and by e the number of errors in the channel.

¹The work of Vladimir Sidorenko is supported by DFG project BO 867/17. He is on leave from Institute for Information Transmission Problems, RAS, Moscow, Russia.

²The work of Christian Senger is supported DFG project BO 867/15.

The decoder of the concatenated code \mathcal{C} consists of an inner decoder and an outer decoder. The inner decoder decodes each column $\mathbf{r}_j^{i,T}$, $j = 1, \dots, n^o$, of the received matrix R using a BMD decoder for \mathcal{C}^i correcting up to $(d^i - 1)/2$ errors and producing either a codeword $\tilde{\mathbf{c}}_j^{i,T}$ or indicating a decoding failure. In case of successful decoding, the correspondent q^{k^i} -ary symbol \tilde{c}_j^o is given an unreliability $\Delta_j = d_H(\tilde{\mathbf{c}}_j^i, \mathbf{r}_j^i)$ and both \tilde{c}_j^o and Δ_j are delivered to the outer decoder. Here, $d_H(\cdot, \cdot)$ denotes the Hamming distance. In case of an inner decoding failure, the symbol \tilde{c}_j^o is considered to be erased which implies the greatest possible unreliability $\Delta_j = d^i/2$.

The inner decoder provides the q^{k^i} -ary vector $\tilde{\mathbf{c}}^o = (\tilde{c}_1^o, \dots, \tilde{c}_{n^o}^o)$ to the outer decoder, where potentially some of the symbols are erased, i.e. replaced by a special erasure symbol. We denote $\tilde{\mathbf{c}}^o \triangleq \mathbf{r}^o = (r_1^o, \dots, r_{n^o}^o)$ to indicate that this is the received vector from point of view of the the outer decoder. In addition to \mathbf{r}^o the outer decoder is provided by the vector $\mathbf{\Delta} = (\Delta_1, \dots, \Delta_{n^o})$ of unreliabilities. The outer decoder should decode the received vector \mathbf{r}^o using the unreliabilities $\mathbf{\Delta}$, i.e. it should reconstruct the transmitted codeword \mathbf{c}^o of the outer code and the corresponding information sequence. This decoding problem is also known as Generalized Minimum Distance (GMD) decoding. *Our aim is to optimize the outer decoder if it is restricted to use the decoder of the outer code only once.*

Let us first assume an outer BMD decoder. It corrects ε errors and τ erasures if $2\varepsilon + \tau \leq d^o - 1$, where the factor 2 can be considered as the *tradeoff rate* between errors and erasures for a BMD decoder. If the BMD decoder simply decodes the vector \mathbf{r}^o without using $\mathbf{\Delta}$ we can guarantee correction up to $e < d^o d^i / 4$ channel errors, where $d^o d^i$ is the designed distance of the concatenated code. This fact was shown by Forney [3]. Forney also suggested multi-trial outer decoding, where in each trial a number of least reliable symbols of \mathbf{r}^o are erased and the obtained vector $\tilde{\mathbf{r}}^o$ is decoded by the outer BMD decoder. This multi-trial decoding allows to correct up to $e < d^o d^i / 2$ channel errors, if the number of trials is sufficiently large. However, in this paper we consider single-trial outer decoders only.

In 1973 Zyablov [4] suggested the following single-trial decoding: First, erase all symbols in \mathbf{r}^o whose unreliabilities exceed the fixed threshold $T = d^i/3$. Then, decode the obtained vector $\tilde{\mathbf{r}}^o$ with a BMD decoder for the outer code. This method allows to correct up to $e < d^o d^i / 3$ channel errors. In 1986, Kovalev [1] proposed a single-trial decoding method, where the threshold T is not fixed, but is selected adaptively as a function of $\mathbf{\Delta}$. His algorithm is able to correct up to $e < 3d^o d^i / 8$ channel errors. Some refinements of Kovalev's and Zyablov's approaches were done by Weber and Abdel-Ghaffar in [5]. We should also mention papers by Sorger [7], and Kötter [8] who suggested interesting modifications of a BMD decoder in such a way that multi-trial decoding of the outer code can be made "in one step".

In this paper we assume a BD decoder for the outer code, which corrects up to $(d^o - 1)/\lambda$ errors in the received vector \mathbf{r}^o . More precisely, we assume that the BD decoder corrects ε errors and τ erasures if

$$\lambda\varepsilon + \tau \leq d^o - 1, \quad (1)$$

where the real number $1 < \lambda \leq 2$ is the tradeoff rate between errors and erasures for the BD decoder.

For example, we can use for outer encoding a Reed–Solomon (RS) code $\mathcal{C}^o(n^o, k^o, d^o)$ over the field $\mathbb{F}_{q^{\ell m}}$ of length $n^o < q^m$ with locators taken from the field \mathbb{F}_{q^m} , where $m, \ell \in \{1, 2, \dots\}$, $lm = k^i$. This code can also be regarded as an ℓ -interleaved RS code [6]. In [2] an efficient algorithm is presented, which allows decoding of ε errors and τ erasures if $\varepsilon \leq (d^o - \tau - 1)\ell/(\ell + 1)$, i.e. \mathbf{r}^o is decoded correctly if (1) is satisfied, where $\lambda = (\ell + 1)/\ell$. The decoder from [2] may fail with probability $P_f(\varepsilon, \tau) \leq \gamma q^{-m[(\ell+1)(\varepsilon_{\max}(\tau)-\varepsilon)+1]}$, where $\gamma \approx 1$ and $\varepsilon_{\max}(\tau) \triangleq (d^o - \tau - 1)\ell/(\ell + 1)$. If $P_f(\varepsilon, \tau)$ is not small enough we can make it negligibly small by slightly decreasing the error correcting radius [6].

Kovalev proposed an adaptive algorithm for $\lambda = 2$. In Section 2 we extend his algorithm for arbitrary λ , $1 < \lambda \leq 2$. In Section 3 we estimate the error correction radius of this extended algorithm and show that the radius quickly approaches $d^o d^i/2$ when $\lambda \rightarrow 1$.

2 Single-trial adaptive decoding

From the inner decoder we have a received word $\mathbf{r}^o = (r_1^o, \dots, r_{n^o}^o)$ together with a vector $\mathbf{\Delta} = (\Delta_1, \dots, \Delta_{n^o})$ of unreliabilities for the components of \mathbf{r}^o , where $0 \leq \Delta_j \leq d^i/2$. Here, we assume w.l.o.g. that the components of \mathbf{r}^o are ordered according to their unreliabilities and hence $\Delta_1 \geq \Delta_2 \geq \dots \geq \Delta_{n^o}$.

The decoder of the outer code fails for \mathbf{r}^o with τ erasures and ε errors in unerased positions if

$$\lambda\varepsilon + \tau > d^o - 1, \quad (2)$$

otherwise outer decoding will be correct (see assumption (1)). Given the number of erasures τ , we denote by $\varepsilon(\tau)$ the minimum number of (unerased) erroneous symbols in the input vector that guarantee to cause a decoding failure. From (2) we get

$$\varepsilon(\tau) = \left\lceil \frac{d^o - \tau - 1}{\lambda} \right\rceil + 1. \quad (3)$$

Let us erase the first and thus least reliable τ components of \mathbf{r}^o and decode the obtained input word $\tilde{\mathbf{r}}^o$ by a decoder for the outer code. The decoder will fail if there were at least $\varepsilon(\tau)$ (unerased) erroneous symbols. What is the minimum number $e_\tau(\mathbf{\Delta})$ of errors in the channel given the vector $\mathbf{\Delta}$ of unreliabilities to create $\varepsilon(\tau)$ (unerased) erroneous symbols in $\tilde{\mathbf{r}}^o$?

To have an integer unreliability Δ_j the channel should spend Δ_j errors if inner decoding of the component r_j^o was correct, and at least $d^i - \Delta_j$ errors otherwise. Consequently, the channel requires the minimum number of errors if the erroneous components r_j^o have minimum possible $d^i - \Delta_j$. This takes place when the $\varepsilon(\tau)$ erroneous components r_j^o are situated immediately after the τ erased (first) positions. We obtain

$$\begin{aligned} e_\tau(\mathbf{\Delta}) &= \sum_{j=1}^{\tau} \Delta_j + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} (d^i - \Delta_j) + \sum_{j=\tau+\varepsilon(\tau)+1}^{n^o} \Delta_j \\ &= \sum_{j=1}^{n^o} \Delta_j + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} (d^i - 2\Delta_j). \end{aligned} \tag{4}$$

Remark 1 This is true for even d^i , in this case Δ_j is always integer since $\Delta_j \in \{0, \dots, d^i/2\}$. In case of odd d^i we can have non-integer $\Delta_j = d^i/2$ and $e_\tau(\mathbf{\Delta})$ assumes a larger value then (4). Later on, we consider $e_\tau(\mathbf{\Delta})$ given by (4) only, despite the results can be slightly improved by methods similar to [5].

Given $\mathbf{\Delta}$, if the number e of errors in the channel satisfies $e < e_\tau(\mathbf{\Delta})$ the decoding of \mathcal{C}^o with τ erasures will be successful. Hence, $e_\tau(\mathbf{\Delta})$ is an error correcting radius for given $\mathbf{\Delta}$ and τ . We are free to select $\tau \in \mathcal{T}$,

$$\mathcal{T} = \{0, \dots, d^o - 1\}. \tag{5}$$

Let us select $\tau = \tau^*$ which maximizes the radius $e_\tau(\mathbf{\Delta})$:

$$\tau^* = \arg \max_{\tau \in \mathcal{T}} e_\tau(\mathbf{\Delta}). \tag{6}$$

As a result we obtain the following algorithm:

Algorithm A. Single-trial adaptive outer decoder

Input. Received vector \mathbf{r}^o with unreliability vector $\mathbf{\Delta}$ from the inner decoder.
Code distances d^i, d^o and parameter $1 < \lambda \leq 2$.

Step 1. Find $\tau^* = \arg \max_{\tau \in \mathcal{T}} \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} (d^i - 2\Delta_j)$, where $\varepsilon(\tau)$ is defined in (3).

Step 2. Decode \mathbf{r}^o with erased first τ^* positions by the BD decoder for the outer code.

Output. Either a codeword of the outer code or a decoding failure.

From Algorithm A we see that the complexity of the proposed adaptive decoder comprises the complexity of the decoder for the outer code and additionally the complexity of Step 1, which is upper bounded by $\mathcal{O}(d^o \log d^o)$.

3 Error correcting radius

The goal of this section is to estimate the error correcting radius of Algorithm A with parameter λ . This means we should find the maximum (real) number $\rho(\lambda)$ such that any number $e < \rho(\lambda)$ of errors in the channel are guaranteed to be corrected by Algorithm A. For a given vector Δ of unreliabilities the error correcting radius $\rho(\lambda)$ of Algorithm A is $e_\tau(\Delta)$, where τ^* is defined by (6) (see also Remark 1). The radius $\rho(\lambda)$ of Algorithm A for all possible Δ can be found as the minimum of $e_\tau(\Delta)$ over all possible Δ as follows:

$$\rho(\lambda) = \min_{\Delta} \max_{\tau \in \mathcal{T}} e_\tau(\Delta). \quad (7)$$

To simplify notations let us replace the unreliabilities Δ_j , $j = 1, \dots, n^o$, by real-valued reliabilities h_j as follows: $h_j = (d^i - 2\Delta_j)/d^i$, where

$$0 \leq h_1 \leq h_2 \leq \dots \leq h_{n^o} \leq 1. \quad (8)$$

The greater the reliability value h_j the more reliable is the symbol r_j^o at the input of the outer decoder.

Definition 1 Denote by $\mathbf{h} = (h_1, \dots, h_{n^o})$ the vector of reliabilities and by \mathcal{H} the set of all possible real-valued vectors \mathbf{h} that satisfy restriction (8).

With these notations we rewrite (4) for $e_\tau(\Delta)$ as

$$e_\tau(\mathbf{h}) = d^i \left(\frac{1}{2} \sum_{j=1}^{n^o} (1 - h_j) + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j \right), \quad (9)$$

and from (7) we have for the error correcting radius

$$\rho(\lambda) = \min_{\mathbf{h} \in \mathcal{H}} \max_{\tau \in \mathcal{T}} e_\tau(\mathbf{h}). \quad (10)$$

Let us further simplify the task of finding $\rho(\lambda)$ and state it as a separate problem. First, notice that in (9) and (10) the parameter τ is selected independently of h_j , $j = d^o + 1, \dots, n^o$. The contribution of these specific h_j into (9) is the sum $\sum_{j=d^o+1}^{n^o} (1 - h_j)$. Hence, to minimize in (10) over \mathbf{h} we should select these h_j to have the maximum possible values $h_j = 1$ and this sum will vanish. As a result the summation $\sum_{j=1}^{n^o}$ in (9) can be replaced by $\sum_{j=1}^{d^o}$. Further, $\sum_{j=1}^{d^o} 1$ is replaced by d^o . Now we can formulate our problem as follows.

Problem 1 For any $1 < \lambda \leq 2$ find the error correcting radius $\rho(\lambda)$

$$\rho(\lambda) = d^i \min_{\mathbf{h} \in \mathcal{H}} \max_{\tau \in \mathcal{T}} f_\tau(\mathbf{h}), \quad (11)$$

where

$$f_\tau(\mathbf{h}) = \frac{1}{2} \sum_{j=1}^{d^o} (1 - h_j) + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j. \tag{12}$$

The set \mathcal{H} is given by Definition 1, $\varepsilon(\tau)$ is defined in (3), the integers d^i and d^o are the minimum distances of the component codes, and \mathcal{T} is specified by (5).

Problem 1 coincides with finding the decoding radius of a single-trial adaptive GMD decoder. For this decoder (with $\lambda = 2$) Kovalev obtained in [1] the following bounds for $\rho(2)$:

$$\frac{d^i}{2} \left(d^o + 1 - \left\lceil \frac{d^o + 1}{4} \right\rceil \right) \leq \rho(2) < \frac{d^i}{2} \left(d^o + 2 - \left\lceil \frac{d^o + 1}{4} \right\rceil \right), \tag{13}$$

from where we get an approximation $\rho(2) \approx 3d^i d^o / 8$. Our goal is to estimate $\rho(\lambda)$ for arbitrary $1 < \lambda \leq 2$. The following theorem gives a lower bound for $\rho(\lambda)$.

Theorem 1 *The error correcting radius $\rho(\lambda)$ of the single-trial adaptive algorithm (solution of Problem 1) with parameter λ satisfies the lower bound*

$$\rho(\lambda) \geq \underline{\rho}(\lambda) \triangleq \frac{d^i}{2} \left(\left\lfloor \frac{d^o - 1}{\lambda} \right\rfloor + \left\lfloor \frac{d^o - \lfloor \frac{d^o - 1}{\lambda} \rfloor - 2}{\lambda} \right\rfloor + 2 \right), \tag{14}$$

where d^i, d^o are the distances of the component codes.

For $\lambda = (\ell + 1) / \ell$ the arguments of the floor operations in (14) are integers if d^o satisfies

$$d^o = s(\ell + 1)^2 + \ell + 2, \quad s = 0, 1, \dots \tag{15}$$

In this case we can simplify (14) by omitting the floor operations and get the following expressions for $\underline{\rho}(\lambda)$:

$$\underline{\rho}(\lambda) = \frac{d^i d^o}{2} \left(1 - \left(\frac{\lambda - 1}{\lambda} \right)^2 + \frac{2\lambda^2 - 3\lambda + 1}{d^o \lambda^2} \right) \gtrsim \frac{d^i d^o}{2} \left(1 - \left(\frac{\lambda - 1}{\lambda} \right)^2 \right). \tag{16}$$

If d^o does not satisfy (15), these expressions give a good approximation for $\underline{\rho}(\lambda)$. We see that for $\lambda = 2$ our results coincide with Kovalev's $\rho(2) \approx 3d^i d^o / 8$. In terms of ℓ we equivalently have

$$\underline{\rho} \left(\frac{\ell + 1}{\ell} \right) = \frac{d^i d^o}{2} \left(1 - \frac{1}{(\ell + 1)^2} + \frac{\ell + 2}{d^o (\ell + 1)^2} \right) \gtrsim \frac{d^i d^o}{2} \left(1 - \frac{1}{(\ell + 1)^2} \right).$$

Theorem 2 *The error correcting radius $\rho(\lambda)$ of the single-trial adaptive algorithm (the solution of Problem 1) with parameter λ satisfies the following upper bound*

$$\rho(\lambda) \leq \bar{\rho}(\lambda) \triangleq \frac{d^i}{\lambda} \left(d^o - 1 - \frac{1}{2} \left\lfloor \frac{d^o - 1}{\lambda} \right\rfloor \right), \quad (17)$$

where $\varepsilon(\tau)$ is defined in (3) and d^i, d^o are the distances of the component codes.

The obtained upper and lower bounds (17) and (14) are nearly tight and the approximation (16) holds for both bounds. Now we additionally show that the bounds are exact if d^o satisfies (15).

Corollary 1 *If $\lambda = (\ell + 1)/\ell$ and d^o satisfies (15), then the error correcting radius $\rho(\lambda)$ is $\rho(\lambda) = \underline{\rho}(\lambda) = \bar{\rho}(\lambda)$.*

References

- [1] S. I. Kovalev, Two classes of minimum generalized distance decoding algorithms, *Probl. Pered. Inform.* 22, 1986, 35-42.
- [2] G. Schmidt, V. R. Sidorenko, and M. Bossert, Collaborative decoding of interleaved Reed–Solomon codes and concatenated code designs, Preprint, available online at ArXiv, [arXiv:cs.IT/0610074](https://arxiv.org/abs/cs.IT/0610074), 2006.
- [3] G. D. Forney Jr., *Concatenated Codes*, Cambridge, MA: MIT Press, 1966.
- [4] V. V. Zyablov, Optimization of concatenated decoding algorithms, *Probl. Pered. Inform.* 9, 1973, 26-32.
- [5] J. H. Weber, K. A. S. Abdel-Ghaffar, Reduced GMD decoding, *IEEE Trans. Inform. Theory* 49, 2003, 1013-1027.
- [6] V. R. Sidorenko, G. Schmidt, M. Bossert, Decoding punctured Reed–Solomon codes up to the Singleton bound, in *Proc. Intern. ITG Conf. Source Channel Coding*, Ulm, Germany, January 2008.
- [7] U. K. Sorger, A new Reed–Solomon code decoding algorithm based on Newton’s interpolation, *IEEE Trans. Inform. Theory* 39, 1993, 358-365.
- [8] R. Kötter, Fast generalized minimum-distance decoding of Algebraic-Geometry and Reed–Solomon codes, *IEEE Trans. Inform. Theory* 42, 1993, 721-737.