On the Minimum Distance of Concatenated Codes and Decoding based on the True Minimum Distance*

Toshiyuki KOHNOSU†, Toshihisa NISHIJIMA†† and Shigeichi HIRASAWA†

†Dept. of Industrial and Management Systems Engineering
Waseda University
Shinjuku-ku, Tokyo 169, Japan

††Dept. of Industrial and Systems Engineering
Hosei University
Koganei-shi, Tokyo 184, Japan

Abstract — **We show some conditions that the minimum distance of concatenated codes is beyond the lower bound. Furthermore a new decoding method is proposed up to the true minimum distance.**

I. Introduction

Concatenated codes proposed by G.D.Forney,Jr.[1] have many remarkable properties from both the theoretical and practical viewpoints. It is known that the minimum distance of a concatenated code is at least the product of the minimum distances of an outer code and an inner code. In this paper, we show some conditions that the minimum distance of concatenated codes is beyond the lower bound. Furthermore a new decoding method is proposed up to the true minimum distance based on Reddy-Robinson algorithm[2] by using the decoding method beyond the BCH bound[3][4].

II. Some Results on the Minimum Distance

A concatenated code over $GF(2)$ is formed from an (N, K, D) code** outer code C over $GF(2^k)$ and an (n, k, d) inner code c over $GF(2)$. The overall concatenated code $\mathcal{C}$ is an $(\mathcal{N}, \mathcal{K}, \mathcal{D})$ code over $GF(2)$, where $\mathcal{N} = nN$, $\mathcal{K} = kK$ and $\mathcal{D} \geq dD$.

If the outer code and the inner code are linear codes, then the concatenated code is also a linear code. Therefore the minimum weight of nonzero codewords equals to the minimum distance.

Theorem 1 *Let C be the outer code over $GF(2^k)$ with parity check matrix H, where $D = 2T + 1$ and one of the rows of H is the vector of length N whose components are all 1's. Let c be the inner code over $GF(2)$, where $d = 2t + 1$. T and t are positive integers. Then the minimum distance $\mathcal{D}$ of the concatenated code $\mathcal{C}$ is at least $dD + 1$, that is, $\mathcal{D} \geq dD + 1$.*

Hereafter we use Reed-Solomon (RS) codes over $GF(2^k)$ as outer codes. Let $\mathrm{RS}_b(N, K)$ denote the (N, K) RS code over $GF(2^k)$ with a generator polynomial $G(x) = \prod_{i=b}^{b+N-K-1}(x - \alpha^i)$, where α is a primitive element of $GF(2^k)$. Let $\mathcal{C}_{\mathrm{RS}_b(N,K)}$ denote the concatenated code with $\mathrm{RS}_b(N, K)$ as an outer code. We obtain the following corollary.

Corollary 1 *The minimum distance of the concatenated codes $\mathcal{C}_{\mathrm{RS}_0(N,N-2T)}$ is at least $dD + 1$.*

We obtain the following results for the case of $K = 1$.

Theorem 2 *Let $b = 1$. Then the minimum distance $\mathcal{D}_{\mathcal{C}_{\mathrm{RS}_1(N,1)}}$ of $\mathcal{C}_{\mathrm{RS}_1(N,1)}$ equals to dD.*

Theorem 3 *Let $b - 1$ and N be relatively prime and $b \neq 1$. Then the minimum distance $\mathcal{D}_{\mathcal{C}_{\mathrm{RS}_b(N,1)}}$ of $\mathcal{C}_{\mathrm{RS}_b(N,1)}$ equals to $\sum_{j=1}^{n} ja_j$, where a_j is the number of codewords of weight j, $j = 0, 1, \cdots, n$, of the (n, k, d) inner code.*

Corollary 2 *If the inner code is not an equi-distance code like simplex codes, then $\mathcal{D}_{\mathcal{C}_{\mathrm{RS}_b(N,1)}} > dD$.*

Thus there is a case that the minimum distance of the concatenated code is beyond the lower bound.

III. Decoding Method up to the True Minimum Distance

We propose a new decoding method which can correct errors up to half of the true minimum distance $dD+\delta$, $\delta > 0$, whereas Reddy-Robinson algorithm corrects errors up to half the lower bound dD on the minimum distance of concatenated codes. Let e be the number of errors. We restrict e as follows‡:

$$\lfloor (dD - 1)/2 \rfloor < e \leq \lfloor (dD + \delta - 1)/2 \rfloor. \tag{1}$$

Lemma 1 *Let $\boldsymbol{c}_i$ and $\hat{\boldsymbol{y}}_i$, $i = 0, 1, \cdots, N - 1$, be the codeword and the estimated codeword by the decoder of i-th inner code, respectively. If a received sequence has e errors, then the following inequality holds:*

$$\sum_{i=0}^{N-1} \frac{d - 2\tau_i}{d} \chi(\hat{\boldsymbol{y}}_i, \boldsymbol{c}_i) > N - D - \frac{\delta}{d}, \tag{2}$$

where

$$\chi(\hat{\boldsymbol{y}}_i, \boldsymbol{c}_i) = \begin{cases} 1, & \hat{\boldsymbol{y}}_i = \boldsymbol{c}_i; \\ -1, & \hat{\boldsymbol{y}}_i \neq \boldsymbol{c}_i, \end{cases} \tag{3}$$

τ_i is the number of errors corrected by the decoder of the i-th inner code.

Eq.(2) is the necessary condition because there are some cases that more than two codewords satisfy Eq.(2) for e errors. So we need to re-encode the codeword $\boldsymbol{C}$ of the outer code by encoder of the inner code and must make sure whether the number of errors is less than $\lfloor (dD + \delta - 1)/2 \rfloor$. When the erasures-and-errors decoder for an outer code can not produce a codeword from a received sequence with e errors at all times, we can apply the decoding method beyond the BCH bound[3][4] for the outer code to get codewords.

Theorem 4 *Let $T = \lfloor (D - 1)/2 \rfloor$. If the erasures-and-errors decoding algorithm based on $T + V$ errors correcting method is executed for the received sequence with e errors at most up to V, where $V = \lfloor (D + \lceil \delta/d \rceil)/2 \rfloor - T$††, then the transmitted codeword can be included in outputs of the decoder of the outer code.*

References

[1] G.D.Forney,Jr., *Concatenated Codes*, M.I.T. Press, Cambridge, Mass., 1966.

[2] S.M.Reddy and J.P.Robinson, "Random error and burst correction by iterated codes," *IEEE Trans. on Information Theory*, vol.IT-18, pp.182–185, 1972.

[3] R.E.Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, Reading, Mass. 1983.

[4] T.Horiguchi, "Errors-and-erasures decoding of Reed-Solomon codes using the decoding algorithm beyond the BCH bound," *IEICE Trans. on Fundamentals*, vol.E73-A, pp.1818–1820, Nov. 1990.

*This work was supported in part by the Ministry of Education under Grant-Aids 07558168 for Science Research and by Waseda University under Grant 96A-259 for Special Research Projects.

**The (N, K, D) denotes the code of length N, dimension K and minimum distance D.

‡ $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x

†† $\lceil x \rceil$ denotes the least integer greater than x.

0-7803-3956-8/97/$10.00 ©1997 IEEE