On the Minimum Distance of Binary Concatenated Codes*

Toshiyuki Kohnosu†, Toshihisa Nishijima‡, and Shigeichi Hiraseawa†, Members

SUMMARY Concatenated codes have many remarkable properties from both the theoretical and practical viewpoints. 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 shall study on a condition that the minimum distance of concatenated codes is beyond the lower bound.

KEY WORDS: concatenated code, minimum distance

1. Introduction

Concatenated codes proposed by G.D. Forney, Jr. [1] have many remarkable properties from both the theoretical and practical viewpoints. They have powerful error correction capability [2] and are also capable of burst error correction. A concatenated code is constructed by combining an outer code and an inner code. 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 shall study on a condition that the minimum distance of concatenated codes is beyond the lower bound.

2. On the Minimum Distance of Binary Concatenated Codes

2.1 Concatenated Codes

The concatenated codes $C$ over $GF(2)$ throughout this paper are restricted to be formed as follows.

Let the outer code be an $(N, K, D)^*$ linear code $C$ over $GF(2^k)$ with parity check matrix $H$, where $D = 2T + 1$ and one of the rows of $H$ is 1, where 1 denotes the vector of length $N$ whose components are all 1’s. And let the inner code be an $(n, k, d)$ linear code $c$ over $GF(2)$ with generator matrix $g$, where $d = 2t + 1$. Here, $T$ and $t$ are positive integers. The overall concatenated code $C$ is an $(N, K, D)$ code over $GF(2)$, where

$N = nN$,

$K = kK$,

and the minimum distance $D$ is at least $dD$, that is,

$D \geq dD$.  

The concatenated codes $C$ are linear codes, so the minimum Hamming weight of the non-zero codewords equals to the minimum Hamming distance.

The construction of a codeword of a concatenated code with a systematic inner code is illustrated in Fig. 1.

2.2 Properties of Binary Expanded Outer Codes

Let $C = (C_0, C_1, \ldots, C_{N-1})$ be a codeword of the outer code, where $C_i \in GF(2^k)$. The codeword $C$ is associated with the polynomial $C(x)$. $C(x)$ is expanded into binary sequences by a basis $\{\beta_0, \beta_1, \ldots, \beta_{k-1}\}$ as follows:

$$C(x) = \sum_{i=0}^{N-1} C_i x^i$$

$$= \sum_{i=0}^{N-1} \left( \sum_{j=0}^{k-1} c_{i,j} \beta_j \right) x^i$$

$$= \sum_{j=0}^{k-1} c_{j}(x) \beta_j,$$

where $c_{i,j} \in GF(2)$ and

$$c_j(x) = \sum_{i=0}^{N-1} c_{i,j} x^i.$$  

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
$C$ & $C_0$ & $C_1$ & $\ldots$ & $C_{N-1}$ \\
\hline
$c_0$ & $c_{0,0}$ & $c_{1,0}$ & $\ldots$ & $c_{N-1,0}$ \\
\hline
$c_1$ & $c_{0,1}$ & $c_{1,1}$ & $\ldots$ & $c_{N-1,1}$ \\
\hline
$c_{k-1}$ & $c_{0,k-1}$ & $c_{1,k-1}$ & $\ldots$ & $c_{N-1,k-1}$ \\
\hline
$c_k$ & $c_{0,k}$ & $c_{1,k}$ & $\ldots$ & $c_{N-1,k}$ \\
\hline
$\vdots$ & $\vdots$ & $\vdots$ & $\ldots$ & $\vdots$ \\
\hline
$c_{n-1}$ & $c_{0,n-1}$ & $c_{1,n-1}$ & $\ldots$ & $c_{N-1,n-1}$ \\
\hline
$\beta_0$ & & & & \\
$\beta_1$ & & & & \\
$\vdots$ & & & & \\
$\beta_{k-1}$ & & & & \\
\hline
\end{tabular}
\caption{A codeword of a concatenated code.}
\end{table}

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

\*The authors received October 18, 1996.

†The authors are with the Department of Industrial and Management Systems Engineering, Waseda University, Tokyo, 169 Japan.

‡The author is with the Department of Industrial and Systems Engineering, Hosei University, Koganei-shi, 184 Japan.

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.

Manuscript received October 18, 1996.

†The authors are with the Department of Industrial and Management Systems Engineering, Waseda University, Tokyo, 169 Japan.

‡The author is with the Department of Industrial and Systems Engineering, Hosei University, Koganei-shi, 184 Japan.

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.
for $0 \leq j \leq k - 1$.

The following lemma holds.

**Lemma 1:** Each binary vector $c_j$ for $0 \leq j \leq k - 1$ has even Hamming weight, where $c_j$ is the vector representation of $c_j(x)$.

**Proof:** Since $H$ has a row vector which is 1 and $CH = 0$,

$$
\sum_{i=0}^{N-1} C_i = 0.
$$

So we have the following identical equations:

$$
\sum_{i=0}^{N-1} C_{i,j} = 0,
$$

for $0 \leq j \leq k - 1$. Since $c_{i,j} \in GF(2)$, each $c_j$ has even Hamming weight.

2.3 The Minimum Distance of the Concatenated Codes $C$

In this section, we suppose that the inner code is a systematic code for simplifying. It is straightforward to extend to nonsystematic codes.

We give the following lemma for binary vectors without proof.

**Lemma 2:** Addition of two binary vectors with even Hamming weight is a binary vector with even Hamming weight.

Let check symbols by encoder of the inner code be $c_j(x)$ for $k \leq j \leq n - 1$, where

$$
c_j(x) = \sum_{i=0}^{N-1} c_{i,j} x^i.
$$

c_j(x)$ for $k \leq j \leq n - 1$ are obtained by linear combination of $c_j(x)$ for $0 \leq j \leq k - 1$ depended on generator matrix $g$ of the inner code.

We have the following theorem on the minimum distance of the concatenated codes $C$.

**Theorem 1:** The minimum distance $D$ of the concatenated codes $C$ is at least $dD + 1$, that is,

$$
D \geq dD + 1.
$$

**Proof:** Each binary vector $c_j$ for $k \leq j \leq n - 1$ has even Hamming weight, since $c_j$ for $0 \leq j \leq n - 1$ are obtained by linear combination of $c_j(x)$ for $0 \leq j \leq k - 1$ and by Lemma 2. As the result, all $c_j$ for $0 \leq j \leq n - 1$ have even Hamming weight. So the minimum Hamming weight of concatenated codes $C$ is even whereas $dD$ is odd. Since the minimum distance $D$ of concatenated codes $C$ is at least $dD$, Theorem 1 holds.

Next we apply $(N, K, D)$ Reed-Solomon (RS) codes over $GF(2^k)$ with generator polynomial $G(x)$ to outer codes, where

$$
G(x) = \prod_{h=0}^{2T-1} (x - \alpha^h),
$$

and $\alpha$ is a primitive element of $GF(2^k)$. When $G(x)$ has $\alpha^0 = 1$ as zeros, $H$ has a row vector of 1 [2]. So we obtain the following corollary.

**Corollary 1:** The minimum distance of the concatenated codes by using RS code which is generated by Eq. (10) as an outer code is at least $dD + 1$.

**Example 1:** Let the outer code be the $(15, 7, 9)$ RS code over $GF(2^4)$ with generator polynomial $G(x) = \prod_{h=0}^{7} (x - \alpha^h)$ and let the inner code be the $(7, 4, 3)$ Hamming code over $GF(2)$. The overall concatenated code is a $(105, 28)$ code over $GF(2)$ and the minimum distance $D$ of the concatenated codes is at least 28 whereas $dD = 27$.

3. Conclusion

We have shown a condition that the minimum distance of concatenated codes is beyond the lower bound. Further studies will be required to obtain the true minimum distance of concatenated codes on the other conditions.

**Acknowledgment**

The authors would like to thank Professor Toshiyasu Matsushima and Mr. Manabu Kobayashi for their fruitful discussions to this work and all the member of Hirasaki Laboratory, Waseda University, for helping us.

**References**