Concatenated codes with convolutional inner codes

Justesen, Jørn; Thommesen, Christian; Zyablov, Viktor

Published in:
I E E E Transactions on Information Theory

Link to article, DOI:
10.1109/18.21249

Publication date:
1988

Document Version
Publisher's PDF, also known as Version of record

Concatenated Codes with Convolutional Inner Codes

JØRN JUSTESEN, CHRISTIAN THOMMESEN, AND VICTOR V. ZYABLOV

Abstract—**We study the minimum distance of concatenated codes with Reed–Solomon outer codes and convolutional inner codes. For suitable combinations of parameters the minimum distance may be lower-bounded by the product of the minimum distances of the inner and outer codes. For a randomized ensemble of concatenated codes we prove a Gilbert–Varshamov-type lower bound.**

I. INTRODUCTION

WE STUDY concatenated codes which are constructed from Reed–Solomon (RS) outer codes and convolutional inner codes. Such codes are of interest in practical coding systems [1] but have not been given much attention in the literature.

We shall consider a concatenated code as a long block code. The convolutional encoder could introduce a slight dependence between successive encoded blocks, but this would be undesirable both from a practical and a theoretical point of view. We may separate the blocks either by introducing a few zero symbols between the RS words (in a practical system, a synchronization pattern would be inserted), or by starting the encoder in a state determined by the last symbols in the RS word. In the first case the rate of the code is reduced, while in the second attention should be given to the possibility that the convolutional encoder may not reach the zero state in a word. For a long RS code and a convolutional code with small memory we can neglect these effects.

For simplicity only binary codes will be considered. The parameters of the outer RS code are (N, K, D), where N is the length, K the dimension, and D the minimum distance. The symbol field GF(2^m) is represented as a linear space of binary vectors of length m, which we shall call bytes. The rate of the outer code is $R = K/N$. The inner code has parameters (ν, κ) where ν is the block length and κ the dimension. The code has memory M blocks, rate $\rho = \kappa/\nu$, and free distance d_∞. In some of the derivations we shall assume that the code is time varying.

Manuscript received June 26, 1986; revised July 8, 1987.

J. Justesen is with the Institute of Circuit Theory and Telecommunication, Technical University of Denmark, Building 343, DK-2800 Lyngby, Denmark.

C. Thommesen is with the Institute of Electronic Systems, Aalborg University Centre, DK-9000 Aalborg, Denmark.

V. V. Zyablov was with the Institute of Circuit Theory and Telecommunication, Technical University of Denmark, Lyngby, Denmark. He is now with the Institute for Problems of Information Transmission, 19 Ermolovoy Street, 101447 Moscow, USSR.

IEEE Log Number 8824279.

We shall compare the fractional minimum distance w of concatenated codes with convolutional inner codes and inner block codes. In Section III we shall find conditions for which w may be lower bounded by the Zyablov bound [2]

$$w \geq (1-R)H^{-1}(1-\rho) \tag{1.1}$$

where H^{-1} is the inverse entropy function. In some cases the minimum distance W may be bounded by

$$W \geq Dd_\infty. \tag{1.2}$$

Such product bounds indicate the quality of concatenated codes when they are used with decoders that decode the inner and outer codes separately. In Section IV, we prove that some concatenated codes have minimum distances that meet the Gilbert–Varshamow bound

$$w \geq H^{-1}(1-R\rho). \tag{1.3}$$

In the outer code interleaving may be used. If I RS codes are interleaved, we shall assume that byte j from the first code is followed by byte j from codes $2, 3, \ldots, I$, and the sequence continues with byte $j+1$ of the first code. The use of interleaving is sometimes explained as a way of adapting the outer code to the bursty error patterns from the inner decoder. We find this description inaccurate since the RS code itself is well suited for correcting burst errors. However, interleaving may be a way of constructing a longer code with little extra complexity, and a longer code will generally have better performance.

In Section III we prove that a bound of the form (1.2) can be achieved if I is chosen properly and $\rho \geq 0.38$. We deduce the rather unexpected result that for lower rates, interleaving is less effective. If it is used, it is necessary to increase the memory to get a bound of the type (1.1).

Each byte representing a symbol from the RS code is encoded as $s = m/\kappa$ blocks of the convolutional code. If s is an integer, we shall assume that the beginning of a byte coincides with the beginning of a block in the convolutional code. However, we shall also consider the case where s is an arbitrary rational number, although for convenience we assume that NIs is an integer. If the outer code is fixed, the performance will generally improve when $M\kappa$ is increased. However, if $M\kappa$ is large enough or s is small enough, the minimum distance satisfies (1.1) and (1.2), and these bounds are not improved by using larger constraint lengths. In Section III, we derive conditions on s/M for long codes so that the lower bounds hold. If κ is

0018-9448/88/0900-1217$01.00

small, it is not important that the blocks of the convolutional code be synchronized with the bytes of the RS code. However, for unit memory codes it has been conjectured that it would be an advantage to match the size of the blocks to the byte length [3]. We prove that in terms of the minimum distance the situation is more complicated. For some intervals of ρ, an integer value of s is advantageous, but at other rates there is no difference. In Section IV it is proved that the Gilbert–Varshamov bound may be attained if both $M\kappa$ and $mN/(M\kappa)$ tend to infinity. Thus this property is not sensitive to the relationship between the symbol size and the constraint length.

In Sections III and IV we derive explicit asymptotic results for long randomly selected codes. For specific inner codes the minimum distance depends on the distance function of the convolutional code. In Section II we derive bounds for specific codes and give examples of good concatenated codes.

II. Lower Bounds on the Minimum Distance of Concatenated Codes With Fixed Inner Codes

In this section we shall derive lower bounds of the product type for concatenated codes with specific inner codes. To obtain bounds on the weight of codewords of the convolutional code, we must know the lengths of the nonzero sequences.

An output sequence from the convolutional encoder is called a codeword if the encoder is started in the zero state and returns to the zero state for the first time at the end of the sequence. The encoded string consists of a number of codewords from the convolutional code separated by zeros. If the input consists of L blocks such that the first and the last are nonzero and there are at most $M-1$ consecutive zero blocks, the output will be a codeword of length $L+M$ blocks.

The encoding of the codewords from the outer code produces a number of codewords from the convolutional code. We give three bounds on the lengths of these codewords.

Lemma 1: If s is an integer and $I=1$, D nonzero bytes from the outer code are encoded as codewords with lengths at least

$$L_j = \begin{cases} s(l_j-2)+M+2, & l_j \geq 2 \\ M+1, & l_j = 1 \end{cases}$$

where

$$\sum_j l_j \geq D.$$

Proof: The nonzero bytes occur in groups of l_j' consecutive bytes, where

$$\sum_j l_j' = D.$$

Each byte consists of s input blocks of length κ, and at least one of these is nonzero. Thus if $l_j' > 1$, the input has length at least $(l_j'-2)s+2$ from the first to the last nonzero block.

If there are at most $M-1$ consecutive zero blocks in the sequence, we get a codeword of length $(l_j'-2)s+M+2$. If $l_j'=1$, the codeword has length at least $M+1$. In those cases we set $l_j = l_j'$. However, if $2s-2 \geq M$, it may happen that the encoder returns to the zero state during the encoding. Thus the string is encoded as several codewords of lengths at least

$$L_{ji} = \begin{cases} s(l_{ji}-2)+M+2, & l_{ji} \geq 2 \\ M+1, & l_{ji} = 1 \end{cases}$$

where

$$\sum_i l_{ji} \geq l_j.$$

On the other hand, if $M > s$, the encoder may not return to the zero state before it reaches a new group of nonzero bytes, and the length of a codeword will be at least

$$L_j = (l_j-2)s + M + 2$$

where

$$l_j \geq \sum_i l_{ji}'.$$

In all cases the lemma follows.

Lemma 2: If s is an integer and $s \geq M$, D nonzero columns of the interleaved outer codes are encoded as codewords with lengths at least

$$L_j = \begin{cases} s(l_j-2)+M+2, & l_j \geq 2 \\ M+1, & l_j = 1 \end{cases}$$

where

$$\sum_j l_j \geq ID$$

if all codewords of the outer codes are nonzero. If at least one outer codeword is zero, each nonzero column is encoded as a codeword of length $\geq M+1$.

Proof: Since we assume $s \geq M$, the convolutional encoder will return to the zero state when the input contains a zero byte. Thus in the case of at least one zero outer codeword the encoder returns to the zero state in each column. If none of the outer codewords are all zeros, there are at least ID nonzero bytes, and the lemma follows from Lemma 1.

Lemma 3: If s is a rational number, $s \geq M$, D nonzero columns of the outer codes are encoded as codewords with lengths at least

$$L_j = \begin{cases} \lfloor (l_j-2)s \rfloor + M + 1, & l_j \geq 2 \\ M+1, & l_j = 1, \end{cases}$$

where

$$\sum_j l_j \geq DI$$

if all codewords of the outer codes are nonzero. If at least one outer codeword is zero, each nonzero column is encoded as a codeword of length $\geq M+1$.

Proof: The difference between the case of integral s and the situation considered here is that one input block may contain a few bits from one byte and extend into the next one. Thus two consecutive nonzero bytes may contain only one nonzero block. Since l_j-2 bytes contain $(l_j-2)s$ blocks, which is not necessarily an integer, the smallest integer larger than $(l_j-2)s$ may be enough to account for the nonzero blocks in l_j nonzero bytes. The rest of the proof follows the proof of Lemmas 1 and 2.

The weight of a codeword of length $n+M$ is at least $\hat{d}_n^r$ [4], which we call the extended row distance. It is important in our derivations that $\hat{d}_n^r$ be an increasing function. If this is not the case, we replace it by a lower bound which is increasing

$$d_n^* = \min_{j \geq n} \hat{d}_j^r.$$

In some cases an approximation of the following type is useful:

$$d_n^* \geq \max\{d_\infty, \alpha n + \beta\}.$$

We can now state a lower bound on the minimum distance of the concatenated code.

Theorem 1: If s is an integer and $s \geq M$ or $I=1$, the minimum distance of the concatenated code satisfies

$$W \geq \min\left\{ Dd_\infty, \sum_j d^*_{s(l_j-2)+2} \right\}$$

where

$$\sum_j l_j \geq DI, \qquad l_j \geq 2.$$

Proof: The theorem follows from Lemma 2 if $s \geq M$, and from Lemma 1 if $I=1$. The minimum weight is not obtained with $l_j=1$.

Note that if $I=1$, the case $l_j=2$ for all j gives $d_2^* D/2$, which is always smaller than $d_\infty D$. Thus a bound of $d_\infty D$ can only be achieved with interleaving. The case $I \geq 2$ and $s < M$ is complicated since some outer codewords may be zero without forcing the inner encoder to the zero state. We will make further comments on this case in Section III. The construction of concatenated codes with inner convolutional codes may be demonstrated by a simple example.

Example 1: The (2,1) code with generator polynomials $(1+D+D^2, 1+D^2)$ has

$$\hat{d}_n^r = \lfloor n/2 \rfloor + 5.$$

The bound of Theorem 1 becomes

$$W \geq \min\left\{ 5D, \sum_j \left(\lfloor sl_j/2 \rfloor - s + 6 \right) \right\}.$$

For $I=1$, the best possible result is $W \geq d_2^* D/2 = 3D$, which is the minimum for $s \geq 6$. The best bound on the relative distance is $w \geq (1-R)/4$, which is obtained with an outer code over GF(2^6). To have $W \geq 5D$, we must have $I \geq 2$ and $Is \geq 10$. Again we get $w \geq (1-R)/4$ with two outer codes over GF(2^5).

Theorem 2: If s is a rational number, $s \geq M$, the minimum distance of the concatenated code satisfies

$$W \geq \min\left\{ Dd_\infty, \sum_j d^*_{\lfloor (l_j-2)s+1 \rfloor} \right\}$$

where

$$\sum_j l_j \geq DI, \qquad l_j \geq 2,\ I \geq 2.$$

Proof: The result follows from Lemma 3.

Note that for $I=1$, $l_j=2$ could give a weight of only $(1/2)Dd_\infty$ if each pair of nonzero bytes is encoded as a codeword of weight d_∞.

Let q_ℓ be the number of strings of length ℓ. We may restate the bound of Theorem 1 as

$$W \geq \min\left\{ Dd_\infty, \sum_{\ell \geq 2} q_\ell d^*_{(\ell-2)s+2} \right\}$$

where

$$\sum_\ell \ell q_\ell \geq DI.$$

If we drop the constraint that q_ℓ be an integer and replace it by $q_\ell \geq 0$, we get a linear programming problem. It follows that the minimum is obtained at a point where only one $q_\ell > 0$, and for this ℓ, $q_\ell = ID/\ell$.

Theorem 3: If s is an integer, $s \geq M$, the minimum distance of the concatenated code satisfies

$$W \geq \min_{\ell \geq 2}\left\{ Dd_\infty, ID\ell^{-1} d^*_{(\ell-2)s+2} \right\}.$$

Remark: If $d_n^* \geq \max\{d_\infty, \alpha n + \beta\}$, we may rewrite this expression as

$$W \geq \min_{\ell \geq 2}\left\{ Dd_\infty, IDs\alpha + DI\ell^{-1}(\beta - 2\alpha(s-1)) \right\}.$$

Proof: Since the minimum with noninteger values of q_ℓ must be less than or equal to the minimum in the original problem, the theorem follows from Theorem 1. The same result holds for $I=1$ and $s < M$.

Theorem 4: If s is a rational number, $s \geq M$, the minimum distance of the concatenated code satisfies

$$W \geq \min_{\ell \geq 2}\left\{ Dd_\infty, ID\ell^{-1} d^*_{\lfloor (\ell-2)s+1 \rfloor} \right\}.$$

Proof: The theorem follows from Theorem 2.

Example 2: The (8,4) partial unit memory code found by Lee [3] has row distances

$$\hat{d}_n^r = \begin{cases} 8, & n=1 \\ 2n+4, & n \geq 2 \end{cases}.$$

From Theorem 3 we get

$$W \geq \min_{\ell \geq 2} \{8D, ID(2\ell s - 4s + 8)/\ell\}.$$

The best bound, $W \geq 8D$, is obtained with $s = 2$ and $I = 2$. Thus two outer codes over GF(2^8) can be used to give a concatenated code with fractional distance

$$w \geq (1 - R)/4.$$

The bound would also be obtained if a (32,16) block code were used as the inner code. In this case we get a powerful concatenated code because the (8,4) code has unusual distance properties. The matching of the block length to the byte size is not so important. If we take three outer codes over GF(2^6), i.e., $I = 3$ and $s = 3/2$, Theorem 4 gives the bound

$$W \geq \min_{\ell \geq 2} \{8D, ID\ell^{-1}(2\lfloor(\ell - 2)3/2\rfloor + 6)\} = 8D$$

with almost the same fractional distance.

III. Minimum Distance Bounds for Long Codes

The sequence $\hat{d}_n^r$ has been studied in earlier papers [4]–[6] because it is directly related to the error probability of Viterbi decoding. For a specific code the row distance may be expressed as the sum of a transient term, a periodic term, and a linear term [5]–[8]. Here the slope of the linear term is determined by the minimum average weight of a loop in the state diagram. For noncatastrophic codes,

$$d_\infty = \min_n \{\hat{d}_n^r\}.$$

For long randomly chosen time-varying codes, $\hat{d}_n^r$ is known [4], [8], and in the following section we shall use these results to study the asymptotic properties of long concatenated codes with fixed outer codes. It was proved in [4] that for unit memory codes,

$$\hat{d}_n^r \geq (n+1)\nu H^{-1}(1 - n\rho/(n+1)).$$

This result may be generalized to other convolutional codes as follows.

Lemma 4: There exist long time-varying convolutional codes with memory M and block length ν for which all extended row distances satisfy

$$\hat{d}_n^r/M\nu \geq (1 + n/M)H^{-1}(1 - \rho/(1 + M/n)).$$

Here it is assumed that M and n are positive integers. The quantity

$$r_n = \rho/(1 + M/n)$$

is the rate of the n'th terminated codes.

It is useful to study the normalized row distance as a function of a positive real variable $\gamma = n/M$. We may interpret the function through Forney's inverse concatenation construction [9]. Let

$$\delta = H^{-1}(1 - r)$$

be the Gilbert–Varshamov bound for block codes. A straight line through $(\rho, 0)$ and $(r, \delta(r))$, where

$$r = \rho/(1 + \gamma^{-1})$$

intersects the ordinate at $(1 + \gamma)\delta(r)$. Thus for small γ the normalized distance decreases. The minimum

$$\delta_c = -\rho/\log(2^{1-\rho} - 1)$$

is Costello's lower bound on the normalized free distance [10]. This minimum occurs for

$$\gamma = r/(\rho - r)$$

where

$$r = 1 - H(1 - 2^{\rho - 1}).$$

For larger γ the row distance increases, and asymptotically

$$\hat{d}_n^r/M\nu \simeq \gamma \cdot \delta(\rho).$$

The bound of Lemma 4 is obtained by considering only the sequence of γ's which are multiples of M^{-1}. Thus for finite M the free distance may be larger than Costello's bound, and for sufficiently low rates $\hat{d}_n^r$ is an increasing function of n for all n.

The increasing lower bound d^* may be approximated by

$$d_n^* = \begin{cases} d_\infty, & \text{for } n \leq Mr/(\rho - r) \\ \hat{d}_n^r, & \text{for } n > Mr/(\rho - r) \end{cases}$$

with

$$r = 1 - H(1 - 2^{\rho - 1}).$$

If the minimum in Theorem 3 occurs for large ℓ, we get the bound

$$W \geq IDs\nu H^{-1}(1 - \rho) \tag{3.2}$$

which coincides with the Zyablov bound [2] for long concatenated codes with block codes of rate ρ as inner codes. Thus we cannot expect to get better results with convolutional codes. We shall study conditions on s that assure that this bound is satisfied. It is interesting to make s large since we obtain an inner code of low complexity in this way.

To determine explicitly when the minimum in Theorem 3 occurs, we replace the variable ℓ by the fractional minimum weight of long codewords in the terminated code

$$\delta = H^{-1}\left(1 - \rho\frac{(\ell - 2)s + 2}{(\ell - 2)s + M + 2}\right). \tag{3.3}$$

The largest value of δ occurs for the critical value

$$\log(1 - \delta) = \rho^{-1},$$

and the smallest value corresponding to large ℓ is

$$H(\delta) = 1 - \rho.$$

We shall determine whether the function in Theorem 3 has a local minimum for δ in this interval.

We consider the function

$$B'(\ell, s, \epsilon, \rho, M) = \ell^{-1}((\ell-2)s+\epsilon+M) \cdot H^{-1}\left(1-\rho\frac{(\ell-2)s+\epsilon}{(\ell-2)s+\epsilon+M}\right).$$

Introducing δ as the independent variable, we get

$$H(\delta) = 1-\rho\frac{n}{n+M}$$
$$n = (\ell-2)s+\epsilon$$
$$n+M = \frac{\rho M}{\rho-1+H(\delta)}$$
$$\ell = \frac{M(1-H(\delta))}{s(\rho-1+H(\delta))} - \frac{\epsilon}{s} + 2$$

and finally,

$$B(\delta, s, \epsilon, \rho, M) = \frac{\rho M \delta s}{(M-2s+\epsilon)(1-H(\delta))+\rho(2s-\epsilon)}. \tag{3.4}$$

A local minimum must satisfy $\partial B/\partial\delta = 0$, which can occur only for

$$(M-2s+\epsilon)(1+\log(1-\delta)) = -\rho(2s-\epsilon).$$

Thus we have at most one value of δ, given by

$$\log(1-\delta) = \frac{-\rho(2s-\epsilon)}{M-2s+\epsilon} - 1 = \frac{(1-\rho)(2s-\epsilon)-M}{M-2s+\epsilon}. \tag{3.5}$$

As s increases, this point approaches the largest value of δ. It may be verified that for smaller values of s we do get a minimum of B. The largest s for which we avoid a local minimum is obtained by introducing the limiting value of δ given by

$$H(\delta) = 1-\rho$$

in (3.5). This yields

$$s_\epsilon = \frac{\frac{1}{2}M(1+\log(1-\delta))}{H(\delta)+\log(1-\delta)} + \frac{\epsilon}{2}, \tag{3.6}$$

or in terms of the rate of the inner code

$$s_\epsilon = \frac{\frac{1}{2}M\left(1+\log\left(1-H^{-1}(1-\rho)\right)\right)}{1-\rho+\log\left(1-H^{-1}(1-\rho)\right)} + \epsilon/2.$$

The function s_0/M is plotted in Fig. 1. As $\rho \to 0$, s_0/M approaches 0.5. For increasing ρ it increases monotonically and is unbounded as $\rho \to 1$. Note that $s_0/M \geq 1$ for $\rho \geq 0.38$. From this analysis we can now derive bounds on parameters of concatenated codes which satisfy the Zyablov bound.

Theorem 5: Concatenated codes exist with long convolutional codes of large memory as inner codes such that

$$W \geq DIs\nu H^{-1}(1-\rho)$$

if $s \leq s_0$ and

$$I \leq \frac{d_\infty}{\nu s H^{-1}(1-\rho)}, \qquad \text{for } \rho \geq 0.38$$
$$I = 1, \qquad \text{for } \rho < 0.38.$$

Proof: For long codes with fixed ν, M and s are large and their ratio may be found from (3.4) with $\epsilon = 0$. If s/M is chosen to be at most s_0/M, it follows from Theorem 3 that

$$W \geq \min\left\{ Dd_\infty, ID \lim_{\ell\to\infty}\left\{\ell^{-1}\hat{d}^r_{\ell s}\right\}\right\}$$

and the Theorem follows from Lemma 4 if $s_0/M \geq 1$. If we neglect integer constraints and take the largest possible value of I, we get the bound $W \geq Dd_\infty$.

For rates < 0.38, M must be greater than s, the length of the symbols in the outer codes. In that case the calculation of the distance of interleaved codes is more difficult. With $I = 1$, the bound of Theorem 5 is at most $Dd_\infty/2$. The reason for this discontinuity in the lower bound may be explained by considering $I = 2$ and M slightly greater than s. If only one of the outer codewords is nonzero, the inner encoder may not return to the zero state, and two nonzero symbols may be encoded as a codeword in the convolutional code of length $\sim 2M$. By Lemma 4 the weight of such a word is at least $2M\nu H^{-1}(1-\rho/2)$, which is smaller than $2d_\infty$. However, this is a weakness of the bound, and the minimum weight would for typical codes be close to $2d_\infty$. However, the bound of Dd_∞ cannot be obtained for low rates.

If we use $\hat{d}^r_n \geq \alpha n + \beta$, s_0 equals $\beta/(2\alpha)$, and I must satisfy $I \leq d_\infty/(s\alpha)$. In Theorem 5 we could use Costello's bound to express d_∞ in terms of ν, M, and ρ.

For unit memory codes the minimum for B does not occur at the point just calculated since δ assumes values from a discrete set. However, if B has a local minimum, B must approach its asymptotic value from below, and for sufficiently large ℓ we get distances below the Zyablov bound. Thus it is still necessary that the local minimum for B does not occur for a finite value of ℓ. Combining Lemma 4 and Theorem 3, we should take $\epsilon = 2$ and $M = 1$ in B.

Theorem 6: Concatenated codes exist with long unit memory codes as inner codes such that

$$W \geq DIs\nu H^{-1}(1-\rho)$$

if

$$s \leq \lfloor s_0 \rfloor + 1$$

and

$$I \leq \frac{d_\infty}{\nu s H^{-1}(1-\rho)}.$$

Proof: The result follows from Theorem 3, Lemma 4, and (3.4). Since we assume here that s is an integer, we must round s_0 to the next smaller integer. This bound for s

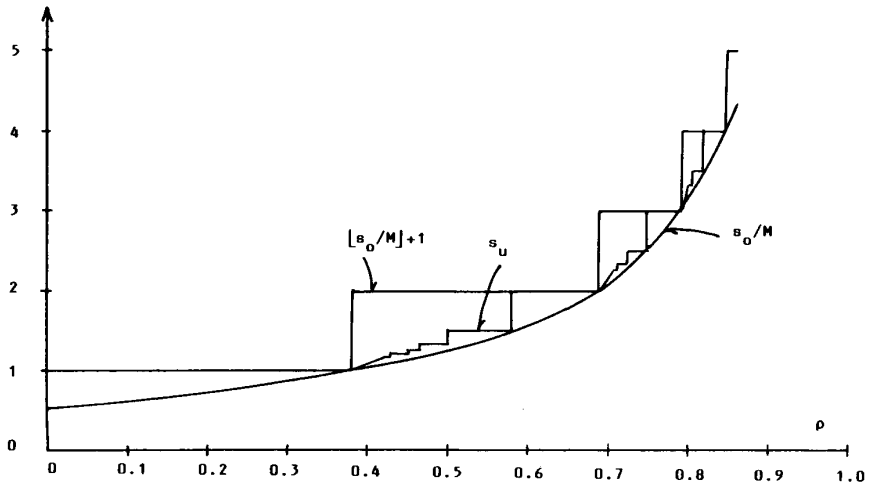

Fig. 1. Relationship between symbol size of outer code and constraint length of inner code.

is indicated in Fig. 1. The free distance can be replaced by the lower bound derived in [4].

Finally, we consider the case where the blocks of the convolutional code are not synchronized with the symbols of the outer code, and s is not necessarily an integer. If ν is very small compared to the symbols of the outer code, it clearly makes no difference if the blocks are synchronized. Thus for multimemory convolutional codes with small ν and large M we can still use Theorem 5. We shall now consider unit memory codes.

In Theorem 4, $(\ell-2)s$ is rounded to the next larger integer. Define $\epsilon(s,\ell)$ by

$$\lfloor(\ell-2)s\rfloor+1=s(\ell-2)+\epsilon(s,\ell)$$

where

$$0<\epsilon(s,\ell)\le 1.$$

We will determine the smallest value of ϵ for a fixed s and use this value in the minimization of B. The most favorable case occurs when s is an integer and $\epsilon(s,\ell)=1$ for all ℓ. In this case we get

$$s\le s_0+\frac{1}{2}.$$

This value applies whenever $s_0+1/2$ is an integer, but the same value can be used for higher rates. In general, if s is chosen to be a rational number, $s=p/q$, where p and q are relatively prime, there are infinitely many ℓ such that

$$\epsilon(s,\ell)=q^{-1}.$$

However, with this value of ϵ we get the constraint

$$s\le s_0+1/(2q).$$

The largest value of s which satisfies these conditions, s_u, is seen to be a piecewise constant function with the set of values $\{i+q^{-1}\}$ for i and q integers. The function s_u is plotted in Fig. 1.

Theorem 7: Concatenated codes exist with long unit memory codes as inner codes such that, without synchronization between the blocks of the inner and outer codes,

$$W\ge IDs\nu H^{-1}(1-\rho)$$

if

$$s=s_u$$

and

$$2\le I\le\frac{d_\infty}{\nu s H^{-1}(1-\rho)}.$$

Proof: The result follows from Theorem 4, Lemma 4, and the previous derivation.

Even though the results of this section are lower bounds on minimum distance, we may interpret the results as indicating useful combinations of the parameters of concatenated codes. In the literature and in practical design there has been some uncertainty about the relationship between the constraint length of the inner codes, the symbol length of the outer code, and the interleaving degree. Theorems 5–7 indicate that these relationships are quite complicated.

For a fixed symbol size $s\kappa$ in the outer code, we may conclude that the constraint length $M\kappa$ can be chosen to be somewhat smaller without negative effects on the minimum distance as long as $\rho>0.38$. For lower rates the block length of unit memory codes should coincide with the symbol length. For multimemory codes of low rates, $M\kappa$ must exceed the symbol length. We find the rather unexpected conclusion that interleaving may lead to codes with lower relative distance unless the constraint length of the inner code is increased to compensate for this effect.

In general, a small degree of interleaving is a useful way of getting a longer code without increasing the complexity much. However, if the outer code has large distance so that the mean value of the number of correctable errors is the

important parameter, interleaving is really only essential for outer codes that are not synchronized with inner unit memory codes.

The advantage of using unit memory codes and of synchronizing the blocks depends on the rate. For rate $1/2$ there is a significant difference between the three cases, whereas this is not the case for $\rho = 2/3$.

Example 3: For $\rho = 1/2$ we obtain the following parameters. For multimemory codes, $s/M \leq 1.25$. If we take the largest possible value, $I = 3$ may be used. In practical systems with an $M = 6$ inner code, $I = 5$ or 8 is used. However, for such a short inner code, $d_\infty/(M\nu)$ is about twice as large as for a long code, and this effect accounts for the difference. The practical value of $s/M = 8/6$ is close to the theoretical value. For unit memory codes we may use $s = 2$, and with this value $I = 2$ can be used in the case of synchronized blocks. Without synchronization, s must be reduced to 1.5.

IV. Minimum Distance Bound for Randomly Selected Inner and Outer Codes

Now we consider concatenated codes where the outer code is a general (N, K) linear code over GF(2^m) without interleaving, and the inner code is a time-varying convolutional code. It is proved that within this class the Gilbert–Varshamov bound can be asymptotically achieved for all rates of the concatenated code when $(M+1)\kappa$ and $mN/((M+1)\kappa)$ tend to infinity, provided that the limits of the inner and outer code rates are properly selected. The condition on the limits is, in a slightly generalized form, the same as the condition in [11, theorem 1, theorem 2] on the limits of the inner and outer code rates that permit the Gilbert–Varshamov bound to be asymptotically achieved for concatenated codes with a Reed–Solomon outer code and time-varying inner block codes. We shall consider ensembles of codes obtained by randomly selecting the inner and outer encoding rules as follows.

The generator matrix $\boldsymbol{G}$ of the outer code is randomly selected with a uniform distribution from the set of all K by N matrices over GF(2^m), where $K \leq N$. Thus for a given information sequence

$$\boldsymbol{u} = [u_1, \ldots, u_k] \in \mathrm{GF}(2^m)^K,$$

the encoded sequence $\boldsymbol{x}$ is given by

$$\boldsymbol{x} = \boldsymbol{u}\boldsymbol{G} \tag{4.1}$$

where the matrix multiplication is over GF(2^m). For every $\boldsymbol{u}$, the $\boldsymbol{x}$ given by (4.1) is a random N row vector over GF(2^m), and if $\boldsymbol{u} \neq \boldsymbol{0}$, each of its $(2^m)^N$ distinct values has the same probability $(2^m)^{-N}$.

When the elements in $\boldsymbol{x}$ are given as m-binary row vectors in a fixed representation of GF(2^m) over GF(2), $\boldsymbol{x}$ becomes an mN binary row vector, and if $\boldsymbol{u} \neq \boldsymbol{0}$, the mN components of $\boldsymbol{x}$ are mutually independent and uniformly distributed. We divide $\boldsymbol{x}$, considered as a binary mN vector, into input blocks of length κ for the convolutional encoder:

$$\boldsymbol{x} = [\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{Ns}] \tag{4.2}$$

where the $\boldsymbol{x}_j$, $1 \leq i \leq Ns$, are binary row vectors of length κ. Thus as in Section II, $s = m/\kappa$ is the number of convolutional code blocks per byte in the outer code, and for convenience, we have assumed Ns to be an integer. Finally, the codeword

$$\boldsymbol{y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{Ns}], \qquad \boldsymbol{y}_t \in \mathrm{GF}(2)^\nu \tag{4.3}$$

in the concatenated code is given by

$$\boldsymbol{y}_t = \boldsymbol{x}_t G_0(t) + \boldsymbol{x}_{t-1} G_1(t) + \cdots + \boldsymbol{x}_{t-M} G_M(t), \quad 1 \leq t \leq Ns \tag{4.4}$$

where $\boldsymbol{x}_t$, $1 \leq t \leq Ns$, is given by (4.2) and (4.1) and $\boldsymbol{x}_0 = \boldsymbol{x}_{-1} = \cdots = \boldsymbol{x}_{1-M} = \boldsymbol{0}$.

The matrix operations in (4.4) are with respect to GF(2), and the matrices

$$\boldsymbol{G}_i(t), \qquad 1 \leq t \leq Ns \text{ and } 0 \leq i \leq M \tag{4.5}$$

are selected randomly, independent of $\boldsymbol{G}$, and mutually independent with a uniform distribution from the set of all binary κ by ν matrices. Thus $\boldsymbol{x}$ is encoded by the inner encoder which is a randomly selected time-varying convolutional encoder, starting in the zero state.

For a fixed information sequence $\boldsymbol{u}$, let

$$P_{\boldsymbol{u}}(\boldsymbol{y}|\boldsymbol{x}) \tag{4.6}$$

denote the conditional probability for the codeword in the concatenated code to be $\boldsymbol{y}$, given that the output from the outer encoder is $\boldsymbol{x}$. The properties of the probability distribution $P_{\boldsymbol{u}}(\cdot|\boldsymbol{x})$ are most easily described in terms of the code trellis [9]. Thus $\boldsymbol{x}$ defines a path through the trellis, reaching the state $[\boldsymbol{x}_{t-M}, \cdots, \boldsymbol{x}_{t-1}]$, $1 \leq t \leq Ns+1$ at time t. The input block $\boldsymbol{x}_t$, $1 \leq t \leq Ns$ at time t determines the branch leading from the state at time t to the state at time $t+1$. Further, the subblock of the convolutional encoder output $\boldsymbol{y}_t$ on that branch is given by (4.4). The zero path is the path through zero states only and corresponds to $\boldsymbol{x} = \boldsymbol{0}$. A branch belongs to the zero path if it leads from the zero state to the zero state. The proof of the result of this section relies on the following lemma.

Lemma 5: Consider, for a fixed information sequence $\boldsymbol{u}$ and a fixed output $\boldsymbol{x}$ from the outer encoder, the conditional distribution $P_{\boldsymbol{u}}(\cdot|\boldsymbol{x})$ on the resulting codeword in the concatenated code. Let λ be the path, defined by $\boldsymbol{x}$, through the trellis. Then the subblocks of the codeword on the branches of λ not belonging to the zero path are mutually independent and uniformly distributed.

Proof: If $\boldsymbol{x} = \boldsymbol{0}$, all branches belong to the zero path and there is nothing to prove. For $\boldsymbol{x} \neq \boldsymbol{0}$, the proof is straightforward [9].

For

$$\Delta = \lceil (M+1)/2 \rceil \tag{4.7}$$

let $\boldsymbol{x}$ be divided into segments containing Δ convolutional code input blocks each, and, in addition, one possibly

empty segment at the end containing fewer blocks. Thus

$$n(\Delta) = \lfloor Ns/\Delta \rfloor \tag{4.8}$$

is the number of segments containing Δ blocks and

$$z_i = [x_{(i-1)\Delta+1}, \cdots, x_{i\Delta}], \qquad 1 \le i \le n(\Delta) \tag{4.9}$$

is the content of the i'th segment.

Let $A(Q)$, $0 \le Q \le n(\Delta)-1$ denote the set of output sequences from the outer encoder for which the contents of precisely Q of the $n(\Delta)-1$ first segments are not exclusively zero blocks. It follows from (4.7) that if, for a sequence $x \in A(Q)$, $z_i \ne \mathbf{0}$, $1 \le i \le n(\Delta)-1$, for the i'th segment of x, then none of the branches on the x-defined path through the trellis determined by the blocks in the next segment z_{i+1} belongs to the zero path. Thus if h, $h \ge 0$, is an integer and $W_H(y)$ denotes the Hamming weight of the word y in the concatenated code, it follows from Lemma 5 that

$$P_u(W_H(y) \le h | x \in A(Q)) \le 2^{-\nu\Delta Q} \sum_{i=0}^{h} \binom{\nu\Delta Q}{i}, \qquad 0 \le Q \le n(\Delta)-1 \tag{4.10}$$

for every information sequence u.

In (4.10) we have adopted the convention

$$\binom{\nu\Delta Q}{i} = 0, \qquad i > \nu\Delta Q.$$

For $u \ne \mathbf{0}$, the probability of $x \in A(Q)$ is given by

$$P_u(x \in A(Q)) = 2^{-(n(\Delta)-1)\kappa\Delta} \binom{n(\Delta)-1}{Q} (2^{\kappa\Delta}-1)^Q$$

and consequently, from (4.10),

$$\begin{aligned} P_u(W_H(y) \le h) &= \sum_{Q=0}^{n(\Delta)-1} P_u(W_H(y) \le h | x \in A(Q)) P_u(x \in A(Q)) \\ &\le \sum_{Q=0}^{n(\Delta)-1} 2^{-\nu\Delta Q} \sum_{i=0}^{h} \binom{\nu\Delta Q}{i} 2^{-(n(\Delta)-1)\kappa\Delta} \\ &\quad \cdot \binom{n(\Delta)-1}{Q} (2^{\kappa\Delta}-1)^Q. \end{aligned} \tag{4.11}$$

With the definitions $a \wedge b = \min\{a, b\}$, $a/0 = \infty$ for $a > 0$ and $0/0 = 0$, we obtain from the inequalities

$$\binom{n(\Delta)-1}{Q} \le 2^{n(\Delta)-1},$$

$$\sum_{i=0}^{h} \binom{\nu Q\Delta}{i} \le 2^{\nu Q\Delta H((h/(\nu Q\Delta)) \wedge 1/2)}$$

and from (4.11)

$$P_u(W_H(y) \le h) \le \sum_{Q=0}^{n(\Delta)-1} \{2^{-\nu Q\Delta[1-H((h/(\nu Q\Delta)) \wedge 1/2)]} \cdot 2^{\rho\nu\Delta[Q-n(\Delta)+1]+n(\Delta)-1}\}, \qquad \text{for } u \ne \mathbf{0}. \tag{4.12}$$

From the union bound it follows that for this ensemble of concatenated codes the minimum distance W satisfies

$$P(W \le h) \le \sum_{u \in \mathrm{GF}(2^m)^K - \{0\}} P_u(W_H(y) \le h). \tag{4.13}$$

By introducing the dimensionless rate $R = K/N$ of the outer code, it follows that

$$2^{mK} = 2^{mNR} = 2^{\kappa sNR} \le 2^{\Delta\nu\rho R(n(\Delta)+1)}$$

and then from (4.12) and (4.13),

$$P(W \le h) \le \sum_{Q=0}^{n(\Delta)-1} \{2^{-\nu Q\Delta[1-H((h/(\nu Q\Delta)) \wedge 1/2))]} \cdot 2^{\rho\nu\Delta[Q+Rn(\Delta)-n(\Delta)+2]+n(\Delta)-1}\}. \tag{4.14}$$

Equation (4.14) is the basic inequality in the proof of Theorem 8. However, to state and prove the theorem, we shall further need the function $\alpha(x)$, defined by

$$\alpha(x) = \begin{cases} 1 - H(1-2^{x-1}), & 0 \le x \le 1 \\ 1, & 1 \le x \end{cases} \tag{4.15}$$

where $(\alpha(x), H^{-1}(1-\alpha(x)))$, $0 \le x \le 1$, is the point where the tangent to $H^{-1}(1-r)$ through $(x, 0)$ touches $H^{-1}(1-r)$ when $H^{-1}(1-r)$, $0 \le r \le 1$, is plotted versus r [11].

In the following we consider infinite sequences (E_j) of concatenated codes where the various parameters depend on j. However, to simplify the notation, we suppress j in these parameters.

Theorem 8: Let ρ_0 and R_0, satisfying

$$0 < \rho_0 \text{ and } 0 < R_0\rho_0 \le \alpha(\rho_0), \tag{4.16}$$

be given. Let an infinite sequence of random ensembles of concatenated codes (E_j), as described earlier with $M \ge 1$, be given such that

$$\lim_{j\to\infty} \rho = \rho_0 \qquad \lim_{j\to\infty} R = R_0 \tag{4.17}$$

and

$$\lim_{j\to\infty} ((M+1)\kappa) = \infty \qquad \lim_{j\to\infty} (mN/((M+1)\kappa)) = \infty. \tag{4.18}$$

Then for every $\epsilon > 0$,

$$\lim_{j\to\infty} P[W/(\nu sN) \le H^{-1}(1-\rho_0 R_0) - \epsilon] = 0. \tag{4.19}$$

Proof: Let ρ_0 and R_0 satisfying (4.16) be given, and let a sequence of ensembles satisfying (4.18) be given. Further, let δ_0 independent of j be given such that $\delta_0 > 0$. With $h = \lfloor \delta_0 \nu n(\Delta)\Delta \rfloor$ and Θ substituted for $Q/n(\Delta)$, we obtain from (4.14)

$$\begin{aligned} P(W/(\nu n(\Delta)\Delta) \le \delta_0) &\le n(\Delta) \sup_{\Theta} \{2^{\nu n(\Delta)\Delta[\rho(\Theta+R-1)-\Theta(1-H(1/2 \wedge \delta_0/\Theta))]}\} \\ &\quad \cdot 2^{\nu n(\Delta)\Delta[2\rho/n(\Delta)+1/(\nu\Delta)-1/(\nu n(\Delta)\Delta)]} \end{aligned} \tag{4.20}$$

where Θ runs through the set $\{0, 1/n(\Delta), \cdots, (n(\Delta)-$

$1)/n(\Delta)\}$ and we have used the fact that

$$1-H\left(\frac{1}{2}\wedge\left(\lfloor\delta_0\nu n(\Delta)\Delta\rfloor/(\nu Q\Delta)\right)\right) \geq 1-H\left(\frac{1}{2}\wedge\left(\delta_0 n(\Delta)/Q\right)\right), \quad \text{for } Q=0,1,\cdots,n(\Delta)-1.$$

Hence by extending Θ to be a continuous variable with range $0\leq\Theta\leq 1$,

$$P\left(W/(\nu n(\Delta)\Delta)\leq\delta_0\right)\leq n(\Delta)\cdot\sup_{0\leq\Theta\leq 1}\left\{2^{\nu n(\Delta)\Delta[\rho(\Theta+R-1)-\Theta(1-H(1/2\wedge\delta_0/\Theta))+2\rho/n(\Delta)+1/(\nu\Delta)]}\right\}. \tag{4.21}$$

To determine under what conditions the optimum in (4.21) is obtained for $\Theta=1$, we introduce the function

$$\varphi(y)=1-H\left(y\wedge\frac{1}{2}\right),\qquad 0\leq y<\infty. \tag{4.22}$$

Then

$$\frac{\partial}{\partial\Theta}\left[\Theta\left(1-H\left(\frac{1}{2}\wedge\frac{\delta_0}{\Theta}\right)\right)\right]=\varphi\left(\frac{\delta_0}{\Theta}\right)-\frac{\delta_0}{\Theta}\varphi'\left(\frac{\delta_0}{\Theta}\right),\quad 0<\Theta. \tag{4.23}$$

By continuity at $\Theta=0$, the optimum in (4.21) is obtained for $\Theta=1$ if

$$\varphi\left(\frac{\delta_0}{\Theta}\right)-\frac{\delta_0}{\Theta}\varphi'\left(\frac{\delta_0}{\Theta}\right)\leq\rho,\qquad 0<\Theta\leq 1. \tag{4.24}$$

The left side of (4.24) can be interpreted geometrically as follows. Let $\varphi(y)$ be plotted versus y. Then $\varphi(\delta_0/\Theta)-(\delta_0/\Theta)\varphi'(\delta_0/\Theta)$ is the ordinate of the point of intersection between the tangent to $\varphi(y)$, with touching point $(\delta_0/\Theta,\varphi(\delta_0/\Theta))$, and the ordinate axis.

Since $\varphi(y)$ is a decreasing and convex function of y, it follows that the left side of (4.24) increases with increasing Θ, and hence (4.24) is equivalent to

$$\varphi(\delta_0)-\delta_0\varphi'(\delta_0)\leq\rho. \tag{4.25}$$

By the fact that both $n(\Delta)$ and $\nu(\Delta)$ tend to infinity with increasing j, it then follows from (4.21) that

$$\lim_{j\to\infty}P\left(W/(\nu n(\Delta)\Delta)\leq\delta_0\right)=0 \tag{4.26}$$

if

$$\rho_0R_0-\varphi(\delta_0)<0 \tag{4.27}$$

and

$$\varphi(\delta_0)-\delta_0\varphi'(\delta_0)\leq\rho_0. \tag{4.28}$$

By the geometric interpretation of $\alpha(x)$ and $\varphi(\delta_0)-\delta_0\varphi'(\delta_0)$, respectively, it follows that (4.26) is also satisfied if

$$\delta_0<H^{-1}(1-\rho_0R_0)\text{ and }\rho_0R_0\leq\alpha(\rho_0).$$

For a given ϵ, $\epsilon>0$, (4.18) is obtained by selecting $\delta_0>0$ such that

$$H^{-1}(1-\rho_0R_0)-\epsilon<\delta_0<H^{-1}(1-\rho_0R_0)$$

(with the trivial case $H^{-1}(1-\rho_0R_0)=0$ excluded), and by using

$$\lim_{j\to\infty}\left(\nu n(\Delta)\Delta/(\nu sN)\right)=1.$$

Remarks: Since (4.16) can be satisfied for every value of ρ_0R_0 such that $0<\rho_0R_0\leq 1$, it is seen from Theorem 8 that the Gilbert–Varshamov bound can be asymptotically achieved for all rates of the concatenated code. It is only required that the number of bits $(M+1)\kappa$ operated on by the inner encoder at a given time, and the number of bits in an outer codeword divided by $(M+1)\kappa$, both tend to infinity. Moreover, no synchronization between the bytes of the outer codewords and the inner encoder is required. For instance, one can fix the rate and block length of the inner code, as is usual with convolutional codes and let the memory, and thereby the constraint length, tend to infinity. If preferable, one can fix the memory $M\geq 1$, letting the block length of the inner code tend to infinity while the inner code rate is approximately fixed. This, for instance, covers the unit memory code point of view. Further, we note that Theorem 8 can be proved when the ensembles of outer codes consist of RS codes with the bytes randomly scrambled.

Finally, Theorem 8 is also valid with $M=0$, that is, with varying block codes as inner codes. The proof, however, is simpler. The segments in (4.9) consist of one inner code information block each, and the inner codewords, corresponding to nonzero information blocks, are mutually independent and uniformly distributed. The rest of the proof is nearly unchanged.

References

[1] Consultative Committee on Space Data Systems, *Telemetry Channel Coding*, 1984.

[2] E. L. Blokh and V. V. Zyablov, *Linejnye Kaskadnye Kody* (Linear Concatenated codes). Moscow, USSR: Nauka, 1982, pp. 56–58.

[3] L.-N. Lee, "Concatenated coding systems employing a unit-memory convolutional code and a byte-oriented decoding algorithm," *IEEE Trans. Commun.* vol. COM-25, pp. 1064–1074, Oct. 1977.

[4] C. Thommesen and J. Justesen, "Bounds on distances and error exponents of unit memory codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 637–649, Sept. 1983.

[5] J. Justesen, "Bounded distance decoding of unit memory codes," in *Proc. IEEE Int. Symp. Inform. Theory*, Les Arcs, France, June 1982.

[6] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun.* vol. COM-19, pp. 751–772, Oct. 1971.

[7] G. K. Huth and C. L. Weber, "Minimum weight convolutional codewords of finite length," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 243–246. Mar. 1976.

[8] F. Hemmati and D. J. Costello, "Asymptomatically catastrophic convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 298–304. May 1980.

[9] G. D. Forney, "Convolutional codes II: Maximum-likelihood decoding," *Inform. Contr.*, vol. 25, pp. 222–266, 1974.

[10] D. J. Costello, "Free distance bounds for convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 356–365, May 1974.

[11] C. Thommesen, "The existence of binary linear concatenated codes with Reed–Solomon outer codes which asymptotically meet the Gilbert–Varshamow bound," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 850–853. Nov. 1983.