Guaranteed Error Correction Rate for a Simple Concatenated Coding Scheme with Single-Trial Decoding

Jos H. Weber, *Member, IEEE,* and
Khaled A. S. Abdel-Ghaffar, *Member, IEEE*

***Abstract*—We consider a concatenated coding scheme using a single inner code, a single outer code, and a fixed single-trial decoding strategy that maximizes the number of errors guaranteed to be corrected in a concatenated codeword. For this scheme, we investigate whether maximizing the guaranteed error correction rate, i.e., the number of correctable errors per transmitted symbol, necessitates pushing the code rate to zero. We show that this is not always the case for a given inner or outer code. Furthermore, to maximize the guaranteed error correction rate over all inner and outer codes of fixed dimensions and alphabets, the code rate of one (but not both) of these two codes should be pushed to zero.**

***Index Terms*—Concatenated codes, decoding strategy, erasure correction, error correction, error detection.**

I. Introduction

In concatenated coding schemes, elementary codes are combined into a powerful code that can be encoded and decoded with relatively low complexity. Concatenated codes have been introduced by Forney [4]. An excellent overview has been provided by Dumer [3].

In this correspondence we study optimization issues concerning the single-trial decoding version of the scheme proposed by Zyablov in [9]. This scheme uses a single inner code, a single outer code, and a fixed single-trial decoding strategy based on bounded distance decoding. Although this may not be the best scheme in terms of performance, it is still worth studying, mainly because of its great simplicity. In particular, the decoder has some attractive low-complexity features compared to other schemes, as will be argued in the following. First of all, it is based on bounded distance decoding techniques only. Furthermore, the inner decoder directly produces the input symbols or erasures for the outer decoder. By contrast, in generalized minimum distance (GMD) based decoding techniques [4], [6], the output symbols of the inner decoder first need to be ordered according to reliability, after which an erasing rule is applied. Finally, in the scheme under consideration, outer decoding is performed only once. By contrast, in multitrial decoding, there are several outer decoders, operating either on the outputs of just as many different inner decoders [9], or on the output of a single inner decoder on which different erasing rules are applied [6]. These outer decoders produce (possibly different) concatenated codewords, one of which being closest to the received sequence, is the final output. For information about multitrial decoding, and many other issues related to concatenated codes, we refer the reader to [3].

In many applications, it is required to design coding schemes for which the alphabets and the dimensions of the codes are fixed. Two criteria play an important role in designing such schemes: the code rate, which is the number of information symbols per transmitted symbol, and the guaranteed error correction rate, which is the number of correctable symbol errors per transmitted symbol. In general, over all codes of fixed dimension and alphabet, the supremum of the guaranteed error correction rate, which is $1/2$, is not attained by any code. Instead, it can only be approached by a sequence of codes whose code rates tend to zero. This is not surprising at all since strong codes, i.e., codes with large Hamming distances, have low rates.

For the simple concatenated coding scheme considered in this correspondence, whose inner and outer codes have fixed alphabets and dimensions, we investigate whether maximizing the guaranteed error correction rate necessarily means pushing the code rate to zero. Surprisingly, we show that if the inner or the outer code are given, then this is not necessarily the case. Furthermore, we show that if the guaranteed error correction rate is maximized over all inner and outer codes of fixed alphabets and dimensions, then the code rate of one, and only one, of these two codes should be pushed to zero. Therefore, to aim at maximizing the guaranteed error correction rate, we should either choose a strong outer code and a weak inner code or *vice versa* (depending on the codes' dimensions and alphabets), and avoid choosing the inner and outer codes to be both weak or both strong! In fact, by choosing the two codes to be weak we lose in correction rate but gain in code rate, while by choosing the two codes to be strong we lose in both correction rate and code rate.

This correspondence is organized as follows. First, in Section II, we describe the scheme under consideration. Next, in Section III, we derive an expression for the maximum number of channel errors which is guaranteed to be corrected by the scheme, and we discuss a slight discrepancy between this result and the corresponding result by Zyablov in [9]. In the same section, we also study the ratio between the number of correctable errors and the (designed) Hamming distance of the concatenated code. Finally, in Section IV, we consider, for given inner and outer code alphabets and dimensions, the guaranteed error correction rate. In particular, we determine all cases for which the optimal guaranteed error correction rate is achieved by finite-length inner/outer codes.

II. The Zyablov Scheme with Single-Trial Decoding

In this section we describe the simple concatenated coding scheme under consideration in this correspondence, which is in fact the single-trial version of the more general scheme proposed by Zyablov in [9]. It uses an outer $[N, K, D]$ block code (i.e., a code of length N, dimension K, and Hamming distance D) over the finite field GF (q^k) and an inner $[n, k, d]$ block code over GF (q). For ease of notation, we introduce $Q = q^k$. The data sequence composed of K Q-ary symbols is first encoded using the outer code to form a sequence of N Q-ary symbols. The inner code is used to map each such symbol to a q-ary sequence of length n. This results in a sequence of Nn q-ary symbols, which we call the overall codeword, that carries Kk q-ary information symbols. The Nn q-ary symbols are then transmitted over a q-ary channel and may suffer from channel errors. The output of the channel is partitioned into N sequences of n q-ary symbols. Each one of these sequences is decoded using the inner code to produce an output sequence of k q-ary symbols, which corresponds to a symbol in GF (Q). As it will be explained later, it may happen that the inner decoder fails to produce a symbol in GF (Q) and produces an erased symbol instead. The N Q-ary symbols/erasures produced by the decoder of the inner code are

Manuscript received November 16, 1997; revised June 7, 1999. The work of K. A. S. Abdel-Ghaffar was supported in part by the National Science Foundation under Grant CCR-96-12354. The material in this correspondence was presented in part at the 1997 IEEE International Symposium on Information Theory, Ulm, Germany, June 29–July 4, 1997, and at the 1998 IEEE International Symposium on Information Theory, Cambridge, MA, August 16–21, 1998.

J. H. Weber is with Delft University of Technology, Faculty of Information Technology and Systems, 2600 GA Delft, The Netherlands (e-mail: j.h.weber@et.tudelft.nl).

K. A. S. Abdel-Ghaffar is with the Department of Electrical and Computer Engineering, University of California at Davis, Davis, CA 95616 USA (e-mail: ghaffar@ece.ucdavis.edu).

Communicated by E. Soljanin, Associate Editor for Coding Techniques.
Publisher Item Identifier S 0018-9448(00)04645-9.

decoded with respect to the outer code to produce a sequence of K Q-ary symbols.

Since the inner code has distance d, it can be used to simultaneously correct up to t and detect up to $d-1-t$ channel errors, where $0 \le t \le \lfloor (d-1)/2 \rfloor$. Such a code is denoted as t-EC $(d-1-t)$-ED (t error correcting and $d-1-t$ error detecting). If there exists an inner codeword which is at distance t or less from the received sequence of n q-ary symbols under consideration, the inner decoder decodes the received sequence into the Q-ary symbol corresponding to that codeword. Otherwise, an erasure is declared. Hence, different decoding strategies can be developed based on the same inner code by varying the parameter t. With regard to the outer decoder, we only assume that it returns the original input sequence of K Q-ary symbols if the number of errors X and the number of erasures Y produced by the inner decoder satisfy $2X + Y \le D - 1$.

III. Optimal Inner Decoding

In designing a concatenated coding scheme, as described in Section II, many choices need to be made that may have an enormous impact on the system performance. One of these choices concerns the choice of the inner decoder. Instead of exploiting the full error correction capability of the inner code (i.e., $t = \lfloor (d-1)/2 \rfloor$), it could also be decided to use this capability only partly (i.e., $t < \lfloor (d-1)/2 \rfloor$), thus leaving more erasures but less errors for the outer decoder. Since more erasures can be corrected than errors, there is a tradeoff problem to be solved in order to determine the optimal choice. In this section, we will determine the choice of t maximizing the number of channel errors in a concatenated codeword for which correction is guaranteed. Further, we will study the ratio between the number of correctable errors and the (designed) distance of the concatenated code.

Let $E(t,d,D)$ be the maximum number of (q-ary) channel errors in the overall codeword for which correction is guaranteed in the concatenated coding scheme described in Section II, i.e., a scheme with an outer code of distance D and a t-EC $(d-1-t)$-ED inner code of distance d. The next proposition gives an explicit expression for $E(t,d,D)$.

Proposition 1: For $0 \le t \le \lfloor (d-1)/2 \rfloor$ and $d, D \ge 1$, we have

$$E(t,d,D) = Dt + D - 1 + \min\{\lfloor D/2 \rfloor (d - 3t - 2), 0\}. \tag{1}$$

Proof: For the decoder of the t-EC $(d-t-1)$-ED inner code to cause a Q-ary symbol error or erasure, at least $d-t$ or $t+1$ channel errors, respectively, have to affect the transmitted q-ary sequence of length n corresponding to that symbol. Further, for the outer code of distance D, correction of X errors and Y erasures is guaranteed if and only if $2X + Y \le D - 1$. Hence

$$E(t,d,D) = \min\{(d-t)X + (t+1)Y - 1 : 2X + Y \ge D\} \tag{2}$$

where the minimum is taken over all nonnegative integers X and Y. For a given X, $(d-t)X + (t+1)Y - 1$ achieves its minimum when $Y = \max\{D - 2X, 0\}$. Hence

$$\begin{aligned} E(t,d,D) &= \min\{(d-t)X + (t+1)(D-2X) - 1\} \\ &= \min\{(d-3t-2)X + Dt + D - 1\} \end{aligned} \tag{3}$$

where the minimum is taken over all integers X such that $0 \le X \le \lfloor D/2 \rfloor$. So the minimum is attained for $X = 0$ in case $d \ge 3t+2$, and for $X = \lfloor D/2 \rfloor$ otherwise. Substituting these values in (3) concludes the proof. □

For our purpose of optimizing the use of an inner code of Hamming distance d, we want to maximize $E(t,d,D)$ over all integers t such that $0 \le t \le \lfloor (d-1)/2 \rfloor$. Let $E(d,D)$ be the maximum value of $E(t,d,D)$ over all integers t with $0 \le t \le \lfloor (d-1)/2 \rfloor$. The following proposition gives an explicit expression for $E(d,D)$ and the values of t for which it is achieved.

Proposition 2: For $d, D \ge 1$, we have

$$E(d,D) = \begin{cases} \left\lfloor \frac{d-1}{2} \right\rfloor, & \text{if } D = 1 \\ \frac{D}{2} \left\lceil \frac{2d}{3} \right\rceil - 1, & \text{if } D \text{ is even} \\ \frac{D-1}{2} \left\lceil \frac{2d}{3} \right\rceil + \left\lceil \frac{d-2}{3} \right\rceil, & \text{if } D \ge 3 \text{ and } D \text{ is odd.} \end{cases} \tag{4}$$

The only choices for t maximizing $E(t,d,D)$ and thus achieving $E(d,D)$ are

$$t = \begin{cases} \left\lfloor \frac{d-1}{2} \right\rfloor, & \text{if } D = 1 \\ \left\lfloor \frac{d}{3} \right\rfloor, \left\lfloor \frac{d}{3} \right\rfloor + 1, \cdots, \left\lfloor \frac{d-1}{2} \right\rfloor, & \text{if } D = 3 \\ \frac{d}{3} - 1, \frac{d}{3}, & \text{if } D \text{ is even and } d \equiv 0 \bmod 3 \\ \left\lfloor \frac{d}{3} \right\rfloor, & \text{otherwise.} \end{cases} \tag{5}$$

Proof: From Proposition 1 it follows that

$$E(t,d,D) = \begin{cases} Dt + D - 1, & \text{if } t \le \left\lfloor \frac{d-2}{3} \right\rfloor \\ \left(D - 3\left\lfloor \frac{D}{2} \right\rfloor\right) t + D - 1 + \left\lfloor \frac{D}{2} \right\rfloor (d-2), & \text{if } t \ge \left\lfloor \frac{d+1}{3} \right\rfloor. \end{cases}$$

Since $E(t,d,1) = t$, the only choice of t that maximizes $E(t,d,D)$ in case $D = 1$ is $t = \lfloor (d-1)/2 \rfloor$. Further, note that for $D \ge 2$, $E(t,d,D)$ is an increasing function of t on the interval $[0, \lfloor (d-2)/3 \rfloor]$. Finally, as a function of t on the interval $[\lfloor (d+1)/3 \rfloor, \lfloor (d-1)/2 \rfloor]$, $E(t,d,D)$ is decreasing if $D = 2$ or $D \ge 4$ and constant if $D = 3$. Hence, for $D \ge 2$ the maximum of $E(t,d,D)$ is achieved for$t = \lfloor (d-2)/3 \rfloor$ or $t = \lfloor (d+1)/3 \rfloor$. Therefore, we consider

$$\begin{aligned} &E(\lfloor (d+1)/3 \rfloor, d, D) - E(\lfloor (d-2)/3 \rfloor, d, D) \\ &\quad = D + \lfloor D/2 \rfloor (d - 2 - 3\lfloor (d+1)/3 \rfloor) \\ &\quad = \begin{cases} D - 2\lfloor D/2 \rfloor \ge 0, & \text{if } D \ge 2 \text{ and } d \equiv 0 \bmod 3 \\ D - \lfloor D/2 \rfloor > 0, & \text{if } D \ge 2 \text{ and } d \equiv 1 \bmod 3 \\ D - 3\lfloor D/2 \rfloor \le 0, & \text{if } D \ge 2 \text{ and } d \equiv 2 \bmod 3. \end{cases} \end{aligned}$$

Note that above equality holds if and only if D is even and $d \equiv 0 \bmod 3$ or $D = 3$ and $d \equiv 2 \bmod 3$. This concludes the proof of (5). Finally, (4) follows by substituting the t from (5) into the expression for $E(t,d,D)$ from Proposition 1. □

In [9] Zyablov presented a concatenated coding scheme with z inner/outer decoders. As stated before, the simple scheme considered in this correspondence can be seen as the $z = 1$ case of Zyablov's scheme. However, the results presented in Proposition 2 slightly differ from the results obtained by substituting $z = 1$ in the relevant formulas from [9]. Zyablov claims the best choice for t in the simple scheme is obtained by rounding off $(d-2)/3$ to the nearest integer. Indeed, $t = (d-2)/3$ maximizes the function $E(t,d,D)$ over all *real* t if $D \ge 2$. However, Propositions 1 and 2 assert that maximizing $E(t,d,D)$ over all *integer* t is not always achieved by the integer closest to $(d-2)/3$. In particular, for $D \ge 3$ odd and $d \equiv 0 \bmod 3$, the option $t = d/3$ indicated by Proposition 2 gives $E(d/3, d, D) = Dd/3$, while Zyablov's choice $t = d/3 - 1$ gives only $E(d/3 - 1, d, D) = Dd/3 - 1$.

In order to study the number of correctable errors as a fraction of the Hamming distance of the concatenated code, we define the functions

$$\phi(t,d,D) = E(t,d,D)/dD \tag{6}$$

and

$$\phi(d,D) = E(d,D)/dD. \tag{7}$$

Note that the denominator dD in (6) and (7) is strictly speaking only a lower bound on the Hamming distance of the concatenated code. Nevertheless, we still call $\phi(t,d,D)$ and $\phi(d,D)$ *correction-to-distance*

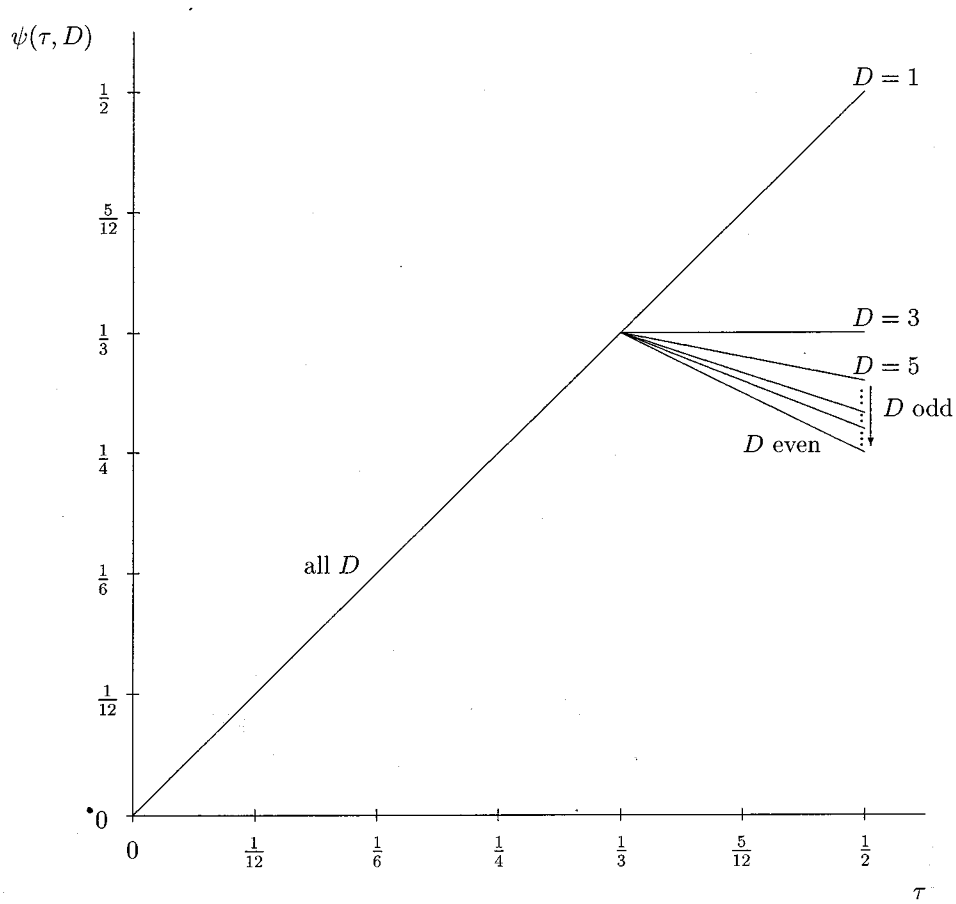

Fig. 1 $\psi(\tau, D)$ for $0 \le \tau < \frac{1}{2}$ and various values of D.

ratios, since the simple (de)coding scheme under consideration does not exploit any advantages a true minimum distance beyond dD might give, and since dD can be considered as a *designed* distance. Next, we determine the asymptotic behavior and the suprema of $\phi(t, d, D)$ and $\phi(d, D)$.

First, we study $\phi(t, d, D)$ for large values of d, while fixing the ratio between t and d. Therefore, we introduce $\tau = t/d$ and define

$$\psi(\tau, D) = \lim_{d \to \infty} \phi(\tau d, d, D). \tag{8}$$

The next result follows immediately from (8), (6), and Proposition 1.

Proposition 3: For $0 \le \tau < (1/2)$ and $D \ge 1$, we have

$$\psi(\tau, D) = \tau + \min\{\lfloor D/2 \rfloor (1 - 3\tau)/D, 0\}. \tag{9}$$

Fig. 1 shows $\psi(\tau, D)$ for $0 \le \tau < \frac{1}{2}$ and various values of D.

Now, we study $\phi(d, D)$. The next six propositions can be derived from an easy analysis of the result (4) in combination with definition (7).

Proposition 4: For $D \ge 1$, we have

$$\lim_{d \to \infty} \phi(d, D) = \begin{cases} \frac{1}{2}, & \text{if } D = 1 \\ \frac{1}{3}, & \text{if } D \ge 2. \end{cases} \tag{10}$$

The result (10) can also be observed from Fig. 1.

Proposition 5: For $D \ge 1$, we have

$$\sup_{d} \phi(d, D) = \begin{cases} \frac{1}{2}, & \text{if } D = 1 \\ \frac{1}{3}, & \text{if } D = 2 \\ \frac{1}{2} - \frac{1}{2D}, & \text{if } D \ge 3 \end{cases} \tag{11}$$

where the supremum is achieved only for

$$\begin{cases} d \to \infty, & \text{if } D = 1, 2 \\ \text{all } d \ge 1, & \text{if } D = 3 \\ d = 2, & \text{if } D \ge 4 \text{ and } D \text{ is even} \\ d = 1, 2 & \text{if } D \ge 5 \text{ and } D \text{ is odd.} \end{cases} \tag{12}$$

Proposition 6: For $d \ge 1$, we have

$$\lim_{D \to \infty} \phi(d, D) = \lceil 2d/3 \rceil / 2d. \tag{13}$$

Proposition 7: For $d \ge 1$, we have

$$\sup_{D} \phi(d, D) = \begin{cases} \frac{1}{2}, & \text{if } d = 1, 2 \\ \frac{3}{8}, & \text{if } d = 4 \\ \frac{1}{d} \left\lfloor \frac{d-1}{2} \right\rfloor, & \text{if } d = 3 \text{ or } d \ge 5 \end{cases} \tag{14}$$

where the supremum is achieved only for

$$\begin{cases} D \to \infty, & \text{if } d = 1, 2, 4 \\ D \to \infty \text{ and all odd } D \ge 1, & \text{if } d = 3, 6 \\ D \to \infty \text{ and } D = 1, & \text{if } d = 5, 8 \\ D = 1, & \text{if } d = 7 \text{ or } d \ge 9. \end{cases} \tag{15}$$

Proposition 8: We have

$$\lim_{D \to \infty} \lim_{d \to \infty} \phi(d, D) = 1/3. \tag{16}$$

Proposition 9: We have

$$\sup_{d,D} \phi(d, D) = 1/2 \tag{17}$$

where the supremum is achieved only for the following three cases:

$$\begin{cases} d=1 & \text{and} \quad D\to\infty, \\ d=2 & \text{and} \quad D\to\infty, \\ d\to\infty & \text{and} \quad D=1. \end{cases} \tag{18}$$

IV. Guaranteed Error Correction Rate

The maximal number of errors in an overall codeword of length nN for which correction is guaranteed is $E(d,D)$. The concatenated scheme can thus correct $E(d,D)/nN$ errors per transmitted q-ary symbol. We call $E(d,D)/nN$ the *guaranteed error correction rate*. In this section, we consider optimization issues with regard to this rate. Throughout, we assume $q, k,$ and K have been given. First, we consider the situation of a given outer code and optimize the guaranteed error correction rate over all possible inner codes. Next, we consider the situation of a given inner code and optimize the guaranteed error correction rate over all possible outer codes. Finally, we consider optimization of the guaranteed error correction rate over inner and outer codes jointly. Of particular interest is whether an optimum is attained for a finite-length inner/outer code or only asymptotically for an infinite sequence of inner/outer codes of increasing lengths.

Let $n_q(k,d)$ be the length of a shortest linear code over GF(q) of dimension k and distance d. An important result which is used in our analysis is the Griesmer bound [5], [7]

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil. \tag{19}$$

Baumert and McEliece [1] proved that for any fixed k and q, equality holds in this bound for all sufficiently large d, i.e., there exists a number $d^*(k,q)$ such that

$$n_q(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil, \qquad \text{for all } \ d \geq d^*(k,q).$$

From this we easily obtain the following results on $n_q(k,d)$:

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \frac{d}{q^i} = \frac{d(1-q^{-k})}{1-q^{-1}}, \tag{20}$$

$$n_q(k,d) = \sum_{i=0}^{k-1} \frac{d}{q^i} = \frac{d(1-q^{-k})}{1-q^{-1}}, \quad \text{if } d \geq d^*(k,q) \ \text{ and } \ d \equiv 0 \bmod q^{k-1} \tag{21}$$

$$n_q(k,d) = d + \sum_{i=1}^{k-1} \frac{d+1}{q^i} = \frac{d(1-q^{-k})+q^{-1}-q^{-k}}{1-q^{-1}}, \quad \text{if } d \geq d^*(k,q) \ \text{ and } \ d \equiv -1 \bmod q^{k-1} \tag{22}$$

$$n_q(k,d) < \frac{d(1-q^{-k})}{1-q^{-1}} + k \quad \text{if } d \geq d^*(k,q) \tag{23}$$

$$\lim_{d\to\infty} \frac{n_q(k,d)}{d} = \frac{1-q^{-k}}{1-q^{-1}}. \tag{24}$$

A. Inner Code Optimization

We now start by considering the situation of a given outer code. Then, the parameters $N, K, D, q,$ and k (and thus $Q=q^k$) are fixed. The inner code is a linear code over GF(q) of dimension k, length n, and distance d. We are interested in optimizing the guaranteed error correction rate over all q-ary inner codes of dimension k. Since N is fixed, it suffices to consider the supremum of

$$\eta_d(q,D,k) = \frac{E(d,D)}{n_q(k,d)} \tag{25}$$

over all positive integers d. Let $\eta(q,D,k)$ denote this supremum. We say that an inner code achieves $\eta(q,D,k)$ if $E/n = \eta(q,D,k)$ where n is the length of the inner code and E is the number of correctable errors in an overall codeword. We say that an infinite sequence of inner codes of increasing lengths asymptotically achieves $\eta(q,D,k)$ if the sequence E/n tends to $\eta(q,D,k)$. Clearly, if no inner code achieves $\eta(q,D,k)$, then there exists a sequence of inner codes that asymptotically achieves $\eta(q,D,k)$. On the other hand, if there exist inner codes that achieve $\eta(q,D,k)$, then it is desirable to specify the shortest length n among all these codes since the overall code rate of the concatenation scheme is $(kK)/(nN)$, where k, K, and N are fixed.

We are now ready to derive an explicit expression for

$$\lim_{d\to\infty} \eta_d(q,D,k)$$

and bounds on $\eta(q,D,k)$.

Proposition 10: For $D \geq 1, q$ is a prime power, and $k \geq 1$, we have

$$\lim_{d\to\infty} \eta_d(q,D,k) = \begin{cases} \frac{1-q^{-1}}{2(1-q^{-k})}, & \text{if } D=1 \\ \frac{D(1-q^{-1})}{3(1-q^{-k})}, & \text{if } D \geq 2. \end{cases} \tag{26}$$

Proof: From (25) and (7) it follows that

$$\eta_d(q,D,k) = \frac{E(d,D)}{n_q(k,d)} = \frac{dD\phi(d,D)}{n_q(k,d)}. \tag{27}$$

Taking the limit as $d\to\infty$ and using (24) and Proposition 4 completes the proof. □

Proposition 11: For $D \geq 1, q$ is a prime-power, and $k \geq 1$, we have

$$\lim_{d\to\infty} \eta_d(q,D,k) \leq \sup_d \eta_d(q,D,k) \leq \frac{D(1-q^{-1})}{1-q^{-k}} \sup_d \phi(d,D) \tag{28}$$

where equality holds in the first inequality if and only if $D \leq 3$ or $D=4$ and $q=3$ and $k\geq 2$; among these cases, the supremum of $\eta_d(q,D,k)$ is achieved for a finite d if and only if $D=3$ or $D=4$ and $q=3$ and $k=2$.

Proof: The first inequality in (28) is trivial, while the second follows from (20) and (7):

$$\eta_d(q,D,k) = \frac{E(d,D)}{n_q(k,d)} \leq \frac{D(1-q^{-1})\phi(d,D)}{1-q^{-k}} \tag{29}$$

for all $d \geq 1$. In order to prove the remaining statements in the proposition, we distinguish between three cases.

Case 1) $D \leq 3$. From Propositions 5 and 10 it now follows that equality holds everywhere in (28) if $D \leq 3$. Hence

$$\eta_d(q,D,k) = \frac{E(d,D)}{n_q(k,d)} = \frac{dD\phi(d,D)}{n_q(k,d)} \leq \lim_{d\to\infty} \eta_d(q,D,k) \tag{30}$$

for all $d \geq 1$. For $D \leq 2$ the inequality in (30) can be shown to be strict for all $d \geq 1$, while for $D=3$ equality holds for all $d \geq d^*(k,q)$ which are multiples of q^{k-1} because of (21).

Case 2) $D \geq 4$ and $q \equiv 1, 2 \bmod 3$. In this case there exists a $\bar{d}$ such that $\bar{d} \geq d^*(k,q)$, $\bar{d} \equiv 2 \bmod 3$, and $\bar{d} \equiv 0 \bmod q^{k-1}$. For this $\bar{d}$, it follows from (21), (4), and Proposition 10 that

$$\begin{aligned} \eta_{\bar{d}}(q,D,k) &= \frac{E(\bar{d},D)}{n_q(k,\bar{d})} = \frac{(1-q^{-1})E(\bar{d},D)}{\bar{d}(1-q^{-k})} \\ &> \frac{D(1-q^{-1})}{3(1-q^{-k})} = \lim_{d\to\infty} \eta_d(q,D,k). \end{aligned} \tag{31}$$

TABLE I
PARAMETERS $[n, k, d]$, $1 \leq k \leq 7$, OF THE SHORTEST INNER BINARY CODES ACHIEVING $\eta(2, D, k)$ FOR $D \geq 3$ AND $\zeta(2, k, K)$ FOR $K \geq 2$

k	achieving $\eta(2, D, k)$	achieving $\zeta(2, k, K)$
1	$[1, 1, 1]$ if $D \geq 3$ is odd $[2, 1, 2]$ if $D \geq 4$ is even	$[1, 1, 1]$
2	$[3, 2, 2]$ if $D \geq 3$	$[3, 2, 2]$
3	$[7, 3, 4]$ if $D = 3$ $[14, 3, 8]$ if $D = 4$ $[4, 3, 2]$ if $D \geq 5$	$[4, 3, 2]$
4	$[15, 4, 8]$ if $D \geq 3$	$[5, 4, 2]$
5	$[31, 5, 16]$ if $D = 3$ $[62, 5, 32]$ if $D = 4$ $[16, 5, 8]$ if $D \geq 5$	$[16, 5, 8]$
6	$[63, 6, 32]$ if $D \geq 3$	$[63, 6, 32]$
7	$[127, 7, 64]$ if $D = 3$ $[254, 7, 128]$ if $D = 4$ $[64, 7, 32]$ if $D \geq 5$	$[64, 7, 32]$

Case 3) $D \geq 4$ and $q \equiv 0 \bmod 3$. In this case there exists a $\bar{d}$ such that $\bar{d} \geq d^*(k, q)$, $\bar{d} \equiv 2 \bmod 3$, and $\bar{d} \equiv -1 \bmod q^{k-1}$. For this $\bar{d}$, it follows from (22) and (4) that

$$\begin{aligned}\eta_{\bar{d}}(q, D, k) &= \frac{E(\bar{d}, D)}{n_q(k, \bar{d})} \\ &= \frac{D\bar{d}/3 + (D-3)/3}{(\bar{d}(1-q^{-k}) + q^{-1} - q^{-k})/(1-q^{-1})} \\ &= \frac{D(1-q^{-1}) + (D-3)(1-q^{-1})/\bar{d}}{3(1-q^{-k}) + 3(q^{-1}-q^{-k})/\bar{d}}. \qquad (32)\end{aligned}$$

Comparing this expression and (26), it follows that the supremum of $\eta_d(q, D, k)$ over d is achieved for a finite value of d and not asymptotically $(d \to \infty)$ if $D \geq 5$ or $q \geq 6$ or $D = 4$ and $q = 3$ and $k = 1$. Further, the supremum of $\eta_d(3, 4, 2)$ over d is achieved both asymptotically $(d \to \infty)$ and for a finite value of d. Finally, the supremum of $\eta_d(3, 4, k)$ over d is achieved only asymptotically $(d \to \infty)$ if $k \geq 3$. □

Table I lists the parameters of the shortest inner binary codes achieving $\eta(2, D, k)$ for $k \leq 7$ and $D \geq 3$. These values of k are considered since $n_2(k, d)$ is known for all d if $k \leq 7$ [8]. As an illustration of the derivation of the entries in the second column of this table, we consider the case $k = 3$. From (28), (26), and (11) we have

$$\frac{4D}{21} \leq \eta(2, D, 3) \leq \frac{2D-2}{7}. \qquad (33)$$

From [8] we know that $n_2(3, d) = d + \lceil d/2 \rceil + \lceil d/4 \rceil$ for all d. In particular $n_2(3, 8) = 14$, and so it follows with (20) and (4) that

$$\eta_d(2, D, 3) = \frac{E(d, D)}{n_2(3, d)} \leq \frac{E(d, D)}{7d/4} \leq \frac{E(8, D)}{14} = \eta_8(2, D, 3) \qquad (34)$$

if $d > 8$ and $D \geq 3$. Hence, for a fixed $D \geq 3$, the maximum of $\eta_d(2, D, 3)$ is attained by some d in the range $1 \leq d \leq 8$. If D is odd, $\eta_d(2, D, 3) = (D-1)/6$, $(D-1)/4$, $D/6$, $(3D-1)/14$, $(2D-1)/10$, $(2D)/11$, $(5D-1)/26$, and $(3D-1)/14$ for $d = 1, \cdots, 8$, respectively. It is easy to check that the smallest d that attains the maximum is 4 if $D = 3$ and 2 if $D \geq 5$ is odd. Thus $[n_2(3, 4) = 7, 3, 4]$ and $[n_2(3, 2) = 4, 3, 2]$ are the parameters of the shortest inner binary codes achieving $\eta(2, D, 3)$ for $D = 3$ and odd $D \geq 5$, respectively. If D is even, $\eta_d(2, D, 3) = (D-2)/6$, $(D-1)/4$, $(D-1)/6$, $(3D-2)/14$, $(2D-1)/10$, $(2D-1)/11$, $(5D-2)/26$, and $(3D-1)/14$ for $d = 1, \cdots, 8$, respectively. It is easy to check that the smallest d that attains the maximum is 8 if $D = 4$ and 2 if $D \geq 6$ is even. Thus $[n_2(3, 8) = 14, 3, 8]$ and $[n_2(3, 2) = 4, 3, 2]$ are the parameters of the shortest inner binary codes achieving $\eta(2, D, 3)$ for $D = 4$ and even $D \geq 6$, respectively.

It can be concluded from Proposition 11 that, for a given q^k-ary $[N, K, D]$ outer code, the guaranteed error correction rate optimization only requires an infinitely long q-ary inner code of dimension k if $D \leq 2$ or $D = 4$ and $q = 3$ and $k \geq 3$. In all other cases, the optimal guaranteed error correction rate is achieved for an inner code of finite length, and so it is not necessary to push the code rate to zero in order to optimize the guaranteed error correction rate. For example, it follows from Table I that for $q = 2$, $k = K = 3$, and a $[7, 3, 5]$ Reed–Solomon code over GF(8) as outer code, the guaranteed error correction rate is optimum when using a binary $[4, 3, 2]$ inner code. This leads to a code rate of $(3 \times 3)/(7 \times 4) = 9/28 = 0.321$ and a guaranteed error correction rate of $E(2, 5)/(4 \times 7) = 4/28 = 0.143$. Note that choosing a binary inner code of dimension 3 with a higher distance (e.g., a binary $[6, 3, 3]$ code [2]) does not improve upon either the code rate of the concatenated code $((3 \times 3)/(6 \times 7) = 9/42 = 0.214)$ or its guaranteed error correction rate $(E(3, 5)/(6 \times 7) = 5/42 = 0.119)$. Ultimately, an infinitely long binary inner code of dimension 3 would lead to a code rate of 0 and a guaranteed error correction rate of $20/147 = 0.136$, where the latter value (derived using Proposition 10) is indeed smaller than the guaranteed error correction rate 0.143 obtained by using the $[4, 3, 2]$ binary inner code.

B. Outer Code Optimization

Next, we continue by considering the situation of a given inner code. Then, the parameters n, k, d, K, and q (and thus $Q = q^k$) are fixed. We are interested in optimizing the guaranteed error correction rate over all Q-ary outer codes of dimension K. Since n is fixed, it suffices to consider the supremum of

$$\theta_D(Q, d, K) = \frac{E(d, D)}{n_Q(K, D)} \qquad (35)$$

over all positive integers D. Let $\theta(Q, d, K)$ denote this supremum. We now derive explicit expressions for both $\lim_{D \to \infty} \theta_D(Q, d, K)$ and $\theta(Q, d, K)$.

Proposition 12: For $d \geq 1$, Q is a prime power, and $K \geq 1$, we have

$$\lim_{D \to \infty} \theta_D(Q, d, K) = \lceil 2d/3 \rceil \frac{1 - Q^{-1}}{2(1 - Q^{-K})}. \qquad (36)$$

Proof: From (35) and (7) it follows that

$$\theta_D(Q, d, K) = \frac{E(d, D)}{n_Q(K, D)} = \frac{dD\phi(d, D)}{n_Q(K, D)}. \qquad (37)$$

Taking the limit as $D \to \infty$ and using (24) and Proposition 6 completes the proof. □

Proposition 13: For $d \geq 1$, Q is a prime-power, and $K \geq 1$, we have

$$\sup_D \theta_D(Q, d, K) = \begin{cases} \lfloor (d-1)/2 \rfloor / K, & \text{if } K = 1 \text{ and } Q \geq 2 \text{ and } d \geq 7 \\ & \text{or } K = 2 \text{ and } Q = 2 \text{ and} \\ & d \geq 15 \text{ and } d \neq 16, 20 \\ \lceil 2d/3 \rceil \frac{1-Q^{-1}}{2(1-Q^{-K})}, & \text{otherwise} \end{cases} \qquad (38)$$

$$\begin{cases} d=1 \text{ and } D\to\infty,\ d=2 \text{ and } D\to\infty, & \\ \quad d\to\infty \text{ and } D=1, & \text{if } k=1 \text{ and } K=1 \\ d=1 \text{ and } D\to\infty,\ d=2 \text{ and } D\to\infty, & \text{if } k=1 \text{ and } K\geq 2 \\ d=2 \text{ and } D\to\infty,\ d\to\infty \text{ and } D=1, & \text{if } k=2 \text{ and } K=1 \text{ and } q=2 \\ d=2 \text{ and } D\to\infty, & \text{if } k=2 \text{ and } K\geq 2 \text{ and } q=2 \\ d\to\infty \text{ and } D=1, & \text{if } k=2 \text{ and } K=1 \text{ and } q\geq 3, \\ & \quad \text{or } k\geq 3 \text{ and } K=1 \\ \text{one or more finite } d \text{ and } D\to\infty, & \text{if } k=2 \text{ and } K\geq 2 \text{ and } q\geq 3 \\ & \quad \text{or } k\geq 3 \text{ and } K\geq 2. \end{cases} \tag{46}$$

where the supremum is achieved for

$$\begin{cases} D=1, & \text{if } K=1 \text{ and } d\geq 7 \text{ and } d\neq 8 \\ & \quad \text{or } K=2 \text{ and } Q=2 \\ & \quad \text{and } d\geq 15 \text{ and } d\neq 16,17,18,20,22,26 \\ D=1 \text{ and } D\to\infty, & \text{if } K=1 \text{ and } d=3,5,6,8 \\ & \quad \text{or } K=2 \text{ and } Q=2 \\ & \quad \text{and } d=9,13,17,18,22,26, \\ D\to\infty, & \text{otherwise.} \end{cases} \tag{39}$$

Furthermore, these D are the only values for which the supremum is achieved, except when $K=1$ and $d=3,6$, or $K\geq 2$ and $Q\equiv 1 \bmod 2$ and $d\equiv 0 \bmod 3$, in which cases the supremum is also achieved for infinitely many finite values of D.

Proof: We start by considering the case $D\geq 2$. It follows from (20), (4), and Proposition 12 that

$$\begin{aligned} \theta_D(Q,d,K) &= \frac{E(d,D)}{n_Q(K,D)} \leq \frac{E(d,D)}{D(1-Q^{-K})/(1-Q^{-1})} \\ &\leq \lceil 2d/3 \rceil \frac{1-Q^{-1}}{2(1-Q^{-K})} = \lim_{D\to\infty} \theta_D(Q,d,K) \end{aligned} \tag{40}$$

for all $D\geq 2$. Note that equality holds in the last inequality in (40) if and only if $d\equiv 0 \bmod 3$ and $D\equiv 1 \bmod 2$. From (19) and (20) it is clear that in order to have equality in the first inequality in (40), it must hold that $D\equiv 0 \bmod Q^{K-1}$. Hence, it can be concluded that for equality to hold everywhere in (40), it is necessary that d is a multiple of 3 and D is both odd and a multiple of Q^{K-1}. With (21) it is thus clear that (infinitely many) finite values of $D\geq 2$ exist for which

$$\theta_D(Q,d,K) = \lim_{D\to\infty} \theta_D(Q,d,K)$$

if and only if either Q is odd and d is a multiple of 3 or Q is even and d is a multiple of 3 and $K=1$.

Based on the preceding analysis for $D\geq 2$, it can be concluded that $\sup_D \theta_D(Q,d,K)$ is achieved for $D=1$ or for $D\to\infty$. Analyzing when the difference

$$\begin{aligned} &\lim_{D\to\infty} \theta_D(Q,d,K) - \theta_1(Q,d,K) \\ &\qquad = \lceil 2d/3 \rceil \frac{1-Q^{-1}}{2(1-Q^{-K})} - \lfloor (d-1)/2 \rfloor / K \end{aligned} \tag{41}$$

is smaller than, equal to, or greater than zero concludes the proof. □

From Proposition 13 it can be concluded that, for a given q-ary $[n,k,d]$ inner code, optimization of the guaranteed error correction rate requires an infinitely long outer code for quite a broad range of cases. However, there are also cases for which the optimal guaranteed error correction is achieved by choosing an outer code with $D=1$, i.e., by having no outer code at all. For example, for $q=2$, $k=3$, $K=1$, and a $[13,3,7]$ binary inner code [2], using no outer code at all leads to a code rate of $3/13=0.231$ and a guaranteed error correction rate of $3/13=0.231$. Using a $[D,1,D]$ outer code over GF (8) with $D\geq 2$ leads to a code rate of $3/(13D)$ and a guaranteed error correction rate of $5/26-1/(13D)$ if D is even and of $5/26-1/(26D)$ if D is odd. Hence, for this example, applying an outer code gives both a lower code rate and a lower guaranteed error correction rate compared to the situation of using no outer code at all. On the other hand, for $q=2$, $k=3$, $K=1$, and a $[7,3,4]$ binary inner code [2], using no outer code at all leads to a code rate of $3/7=0.429$ and a guaranteed error correction rate of $1/7=0.143$. Using a $[D,1,D]$ outer code over GF (8) with $D\geq 2$ leads to a code rate of $3/(7D)$ and a guaranteed error correction rate of $3/14-1/(7D)$ if D is even and of $3/14-1/(14D)$ if D is odd. Hence, for this example, applying an outer code with $D\geq 3$ gives a higher guaranteed error correction rate compared to the situation of using no outer code. Ultimately, the optimal guaranteed error correction rate $3/14=0.214$ is achieved for $D\to\infty$.

C. Joint Inner and Outer Code Optimization

Finally, we consider the joint optimization of inner and outer codes for given q, k, and K (and thus $Q=q^k$). For any d and D, the guaranteed error correction rate is then optimized by choosing an inner code of length $n_q(k,d)$ and an outer code of length $n_{q^k}(K,D)$. Therefore, we introduce the function

$$\zeta_{d,D}(q,k,K) = \frac{E(d,D)}{n_q(k,d)n_{q^k}(K,D)}. \tag{42}$$

Let $\zeta(q,k,K)$ denote the supremum of $\zeta_{d,D}(q,k,K)$ over all positive integers d and D. We now derive an explicit expression for

$$\lim_{D\to\infty} \lim_{d\to\infty} \zeta_{d,D}(q,k,K)$$

and bounds on $\zeta(q,k,K)$.

Proposition 14: For q is a prime power and $k,K\geq 1$, we have

$$\lim_{D\to\infty} \lim_{d\to\infty} \zeta_{d,D}(q,k,K) = \frac{1-q^{-1}}{3(1-q^{-kK})}. \tag{43}$$

Proof: From (42) and (7) it follows that

$$\zeta_{d,D}(q,k,K) = \frac{E(d,D)}{n_q(k,d)n_Q(K,D)} = \frac{dD\phi(d,D)}{n_q(k,d)n_Q(K,D)}. \tag{44}$$

Taking the limits as $d\to\infty$ and $D\to\infty$ and using (24) two times and Proposition 8 completes the proof. □

Proposition 15: For q a prime power and $k,K\geq 1$, we have

$$\frac{1-q^{-1}}{3(1-q^{-kK})} < \sup_{d,D} \zeta_{d,D}(q,k,K) \leq \frac{1-q^{-1}}{2(1-q^{-kK})}. \tag{45}$$

where equality holds in the latter inequality if and only if $K=1$ or $k=1$ or $k=2$ and $q=2$; the supremum is achieved only for the conditions in (46), shown at the top of this page.

Proof: With (20) and Proposition 9 it follows that

$$\begin{aligned}\zeta_{d,D}(q,k,K) &= \frac{E(d,D)}{n_q(k,d)n_Q(K,D)} = \frac{dD\phi(d,D)}{n_q(k,d)n_Q(K,D)}\\ &\le \frac{(1-q^{-1})\phi(d,D)}{1-q^{-kK}} \le \frac{1-q^{-1}}{1-q^{-kK}}\sup_{d,D}\phi(d,D)\\ &= \frac{1-q^{-1}}{2(1-q^{-kK})}\end{aligned} \tag{47}$$

for all $d, D \ge 1$, which proves the upper bound in (45). From Proposition 9 it follows that equality holds in the second inequality in (47) if and only if $d = 1$ and $D \to \infty$ or $d = 2$ and $D \to \infty$ or $d \to \infty$ and $D = 1$. From $n_q(k,1) = k$, $n_q(k,2) = k+1$, and (24), it follows that, among these three cases, equality holds in the first inequality in (47) if and only if $K = 1$ or $k = 1$ or $k = 2$ and $q = 2$. Also, for these parameters the only values for d and D achieving the supremum are indeed as given in (46).

In the rest of this proof we consider the cases in which the second inequality in (45) is strict, i.e., the cases in which $K \ge 2$ and $k = 2$ and $q \ge 3$ or $K \ge 2$ and $k \ge 3$. If q is not a multiple of 3, then there exists a $\bar{d}$ such that $\bar{d} \ge d^*(k,q)$, $\bar{d} \equiv 2 \bmod 3$, and $\bar{d} \equiv 0 \bmod q^{k-1}$. For this $\bar{d}$, it follows from (21), (24), and Proposition 6 that

$$\begin{aligned}\zeta_{\bar{d},\infty}(q,k,K) &= \lim_{D\to\infty}\frac{\bar{d}D\phi(\bar{d},D)}{n_q(k,\bar{d})n_Q(K,D)} = \frac{\lceil 2\bar{d}/3\rceil(1-q^{-1})}{2\bar{d}(1-Q^{-K})}\\ &= \frac{(\bar{d}+1)(1-q^{-1})}{3\bar{d}(1-q^{-kK})} > \frac{1-q^{-1}}{3(1-q^{-kK})}.\end{aligned} \tag{48}$$

If q is a multiple of 3, then there exists a $\bar{d}$ such that $\bar{d} \ge d^*(k,q)$ and $\bar{d} \equiv -1 \bmod q^{k-1}$. For this $\bar{d}$, it follows from (22), (24), and Proposition 6 that

$$\begin{aligned}\zeta_{\bar{d},\infty}(q,k,K) &= \lim_{D\to\infty}\frac{\bar{d}D\phi(\bar{d},D)}{n_q(k,\bar{d})n_Q(K,D)}\\ &= \frac{\lceil 2\bar{d}/3\rceil(1-q^{-1})(1-Q^{-1})}{2(\bar{d}(1-q^{-k})+q^{-1}-q^{-k})(1-Q^{-K})}\\ &> \frac{(\bar{d}+1)(1-q^{-1})(1-q^{-k})}{3(\bar{d}(1-q^{-k})+1-q^{-k})(1-q^{-kK})}\\ &= \frac{1-q^{-1}}{3(1-q^{-kK})}.\end{aligned} \tag{49}$$

This completes the proof of the lower bound in (45).

Finally, note that

$$\sup_{d,D}\zeta_{d,D}(q,k,K) = \sup_{d}\left\{\frac{1}{n_q(k,d)}\sup_{D}\theta_D(Q,d,K)\right\} \tag{50}$$

and observe from Proposition 13 that $\sup_D \theta_D(Q,d,K)$ is achieved for $D \to \infty$ in case $K \ge 2$ and $k = 2$ and $q \ge 3$ or $K \ge 2$ and $k \ge 3$. Furthermore, no finite D achieves this supremum, except when q is odd and d is a multiple of 3. It follows from (20) and (4) that

$$\zeta_{d,D}(q,k,K) = \frac{E(d,D)}{n_q(k,d)n_Q(K,D)} \le \frac{1-q^{-1}}{3(1-q^{-kK})} \tag{51}$$

if $D \ge 2$ and d is a multiple of 3, and that

$$\zeta_{d,1}(q,k,K) = \frac{E(d,1)}{n_q(k,d)n_Q(K,1)} < \frac{1-q^{-1}}{2K(1-q^{-k})} < \frac{1-q^{-1}}{3(1-q^{-kK})} \tag{52}$$

if $q \ge 3$. The latter inequality in (52) follows by observing that

$$2K(1-q^{-k}) \ge 4(1-3^{-2}) = 32/9 > 3(1-q^{-kK}). \tag{53}$$

Hence, it can be concluded that $\sup_{d,D}\zeta_{d,D}(q,k,K)$ is only achieved for $D \to \infty$ and one or more finite d in case $K \ge 2$ and $k = 2$ and $q \ge 3$ or $K \ge 2$ and $k \ge 3$. □

Table I lists the parameters of the shortest inner binary codes achieving $\zeta(2,k,K)$ for $k \le 7$ and $K \ge 2$. (Note that no such codes exist if $K = 1$ and $k \ge 3$.) From Proposition 15, D should tend to infinity to achieve $\zeta(2,k,K)$. Indeed, except in case $k = 4$, the code parameters are identical to those listed in the second column of the table as the parameters of the shortest inner binary codes achieving $\eta(2,D,k)$ as D tends to infinity. We choose the exceptional case $k = 4$ as an illustration of the derivation of the entries in the third column of this table. Proposition 6 and (24) imply that

$$\begin{aligned}\zeta_{d,\infty}(2,4,K) &= \lim_{D\to\infty}\frac{dD\phi(d,D)}{n_2(4,d)n_{16}(K,D)}\\ &= \frac{15}{32(1-16^{-K})}\frac{\lceil 2d/3\rceil}{n_2(4,d)}.\end{aligned} \tag{54}$$

Furthermore, from [8] we know that

$$n_2(4,d) = d + \lceil d/2\rceil + \lceil d/4\rceil + \lceil d/8\rceil$$

for all d. Thus maximizing $\zeta_{d,\infty}(2,4,K)$ over all d is equivalent to maximizing

$$f_d = \frac{\lceil 2d/3\rceil}{d + \lceil d/2\rceil + \lceil d/4\rceil + \lceil d/8\rceil} \tag{55}$$

over all d. Clearly, for $d \ge 9$

$$f_d \le \frac{2(d+1)/3}{d+d/2+d/4+d/8} = \frac{16}{45}\left(1+\frac{1}{d}\right) < \frac{16}{45}\left(1+\frac{1}{8}\right) = f_8. \tag{56}$$

Hence, the maximum of f_d is attained by some d in the range $1 \le d \le 8$. It is easy to see that $f_d = 1/4, 2/5, 2/7, 3/8, 4/11, 1/3, 5/14, 2/5$ for $d = 1, \cdots, 8$, respectively. Therefore, the smallest value of d that maximizes f_d and $\zeta_{d,\infty}(2,4,K)$ is 2. However, we should notice that $d = 2$ does not maximize $\zeta_{d,D}(2,4,K)$, which is equivalent to maximizing $\eta_d(2,D,4)$, for any fixed finite integer D. The smallest such d is actually 8 if $D \ge 3$. In fact, $\eta_2(2,D,4) = (D-1)/5$ and $\eta_8(2,D,4) = (D-1/3)/5$ for $D \ge 3$.

We can conclude from Proposition 15 that in order to optimize the guaranteed error correction rate over all q-ary inner codes of dimension k and all q^k-ary outer codes of dimension K, it is necessary to choose an inner or outer code of infinite length. However, not both the outer and the inner codes should be infinitely long, since that leads to a suboptimal guaranteed error correction rate!

REFERENCES

[1] L. D. Baumert and R. J. McEliece, “A note on the Griesmer bound,” *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 134–135, Jan. 1973.

[2] A. E. Brouwer and T. Verhoeff, “An updated table of minimum-distance bounds for binary linear codes,” *IEEE Trans. Inform. Theory*, vol. 39, pp. 662–677, Mar. 1993.

[3] I. I. Dumer, “Concatenated codes and their multilevel generalizations,” in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998, ch. 23.

[4] G. D. Forney Jr., *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.

[5] J. H. Griesmer, “A bound for error-correcting codes,” *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.

[6] S. I. Kovalev, “Two classes of minimum generalized distance decoding algorithms,” *Probl. Pered. Inform.*, vol. 22, no. 3, pp. 35–42, 1986.

[7] G. Solomon and J. J. Stiffler, “Algebraically punctured cyclic codes,” *Inform. Contr.*, vol. 8, pp. 170–179, 1965.

[8] H. C. A. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," *Discr. Math.*, vol. 33, pp. 197–207, 1981.

[9] V. V. Zyablov, "Optimization of concatenated decoding algorithms," *Probl. Pered. Inform.*, vol. 9, no. 1, pp. 26–32, 1973.

The Undetected Error Probability Threshold of m-out-of-n Codes

Fang-Wei Fu, Torleiv Kløve, *Senior Member, IEEE*, and Shu-Tao Xia

***Abstract*—The well-known m-out-of-n code Ω_n^m consists of all binary vectors of length n and weight m. It is known that it is good for error detection (in the technical sense, that is, the probability of undetected error $P_{\rm ud}(\Omega_n^m, p) \le P_{\rm ud}(\Omega_n^m, 1/2)$ for all $p, 0 \le p \le 1/2$) only for a few small values of m and n. It is therefore of interest to determine (bounds for) the threshold in general, that is, find the range of bit-error probabilities p for which $P_{\rm ud}(\Omega_n^m, p) \le P_{\rm ud}(\Omega_n^m, 1/2)$. In this correspondence such bounds are given.**

***Index Terms*—Error detection, m-out-of-n codes, undetected error probability threshold.**

The well-known m-out-of-n code Ω_n^m consists of all binary vectors of length n and weight m. The m-out-of-n codes have been widely used as the error-detecting codes in the digital communication systems with feedback, such as the automatic-repeat-request (ARQ) error-control system. The undetected error probability of an error-detecting code is one of the major parameters for evaluating the efficiency of ARQ error-control system. For a general introduction to the theory of the probability of undetected error for codes, we refer the reader to [3] and its references. Wang, Yang, and Zhang, [5]–[10] studied the codes Ω_n^m for error detection.

Let C be a binary code of length n and size M. When the code C is used for error detection on a binary-symmetric channel with symbol error probability p, the undetected error probability is denoted by $P_{\rm ud}(C, p)$. A general rule of thumb is that to use C for error detection, we want

$$P_{\rm ud}(C, p) \le P_{\rm ud}(C, 1/2) \tag{1}$$

mainly because this gives a simple upper bound on $P_{\rm ud}(C, p)$ for all $p \in [0, 1/2]$. Therefore, if (1) is satisfied for all $p \in [0, 1/2]$, the code C is called *good* for error detection. However, many codes are not good in this sense. On the other hand, p is usually small in most practical applications and (1) may well be satisfied for the actual values of p. Therefore, we consider the threshold of C (introduced in [2]), which is defined by

$$\theta(C) = \max\left\{ p' \in [0, 1/2] \;\middle|\; \begin{array}{c} P_{\rm ud}(C, p) \le P_{\rm ud}(C, 1/2) \\ \text{for all } p \in [0, p'] \end{array} \right\}.$$

For $p \le \theta(C)$ the bound (1) is still valid. In particular, C is good for error detection if and only if $\theta(C) = 1/2$. Note that $\theta(C)$ is a root of the equation $P_{\rm ud}(C, p) = P_{\rm ud}(C, 1/2)$ and it is the smallest root in the interval (0, 1/2] except in the rare cases when $P_{\rm ud}(C, p)$ happens to have a local maximum for this smallest root (this is not the case for Ω_n^m).

It is easy to show and well known that

$$P_{\rm ud}(\Omega_n^m, p) = \sum_{i=1}^{m} \binom{m}{i} \binom{n-m}{i} p^{2i} (1-p)^{n-2i}. \tag{2}$$

In particular, $P_{\rm ud}(\Omega_n^m, p) = P_{\rm ud}(\Omega_n^{n-m}, p)$ for all n, m, and p. Therefore, we can restrict our attention to m such that $1 \le m \le n/2$. Wang *et al.* [5]–[10] showed that Ω_n^m is good for error detection exactly for the following values of (n, m) with $1 \le m \le n/2$: $(2, 1)$, $(3, 1)$, $(4, 1)$, $(4, 2)$, $(5, 2)$, $(6, 3)$, $(7, 3)$, $(8, 4)$. Another proof of this fact is given in [1].

The goal of this correspondence is to estimate $\theta(\Omega_n^m)$. We start with a heuristic argument for approximations of $\theta(\Omega_n^m)$. We will then prove one such approximation. We use the notations

$$\Psi = \Psi(n, m) = P_{\rm ud}(\Omega_n^m, 1/2) = \frac{\binom{n}{m} - 1}{2^n}$$

$$\psi = \psi(n, m) = \left(\frac{\Psi(n, m)}{m(n-m)} \right)^{1/2}.$$

From (2) we see that $\theta = \theta(\Omega_n^m)$ is the smallest positive root of the equation

$$m(n-m)\psi^2 = \sum_{i=1}^{m} \binom{m}{i} \binom{n-m}{i} \theta^{2i} (1-\theta)^{n-2i}.$$

In particular, if $\theta = \theta(\Omega_n^m)$ is small, then $\theta \approx \psi$.

Consider the corresponding general equation

$$m(n-m)y^2 = \sum_{i=1}^{m} \binom{m}{i} \binom{n-m}{i} p^{2i} (1-p)^{n-2i} \tag{3}$$

where p and y are variables. Solving for p, we get p as a function of y, and it can be expressed as a power series

$$p = \sum_{j=1}^{\infty} s_j(n, m)\, y^j. \tag{4}$$

The simplest way to determine the coefficients $s_j(n, m)$ is to substitute (3) in (4) and compare coefficients. We get the following initial terms of (4):

$$\begin{aligned} p = y + \frac{n-2}{2}\, y^2 + \frac{3n^2 - 9n + 7 - m(n-m)}{8}\, y^3 \\ + \frac{(4n^2 - 11n + 9 - 3m(n-m))\,(n-1)}{12}\, y^4 + \cdots. \end{aligned} \tag{5}$$

Note that it is not *a priori* clear if this expansion converges for $y = \psi$ and we have no proof that it does. If it does, we expect to get a good approximation to θ by taking the first few terms in the expansion. A heuristic argument indicates that the expansion converges at least for $|y| < 2/(en)$ and we will show that $\psi < (32/(\pi n^5))^{1/4} < 2/(en)$.

Manuscript received June 21, 1999; revised December 30, 1999. This workwas supported in part by the Chinese Foundation of Institution of Higher Education for Doctoral Program, National Natural Science Foundation of China, and The Norwegian Research Council. The material in this correspondence was presented in part at the 5th International Symposium on DSP for Communication Systems, Perth, Australia, February 1–4, 1999.

F.-W. Fu is with the Department of Mathematics, Nankai University, Tianjin 300071, China.

T. Kløve is with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway.

S.-T. Xia was with the Department of Mathematics, Nankai University, Tianjin, China. He is now with Tianjin Zhenglian Information Engineering Company Ltd., Tianjin, China.

Communicated by A. M. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)04291-7.