Focused Codes for Channels with Skewed Errors

THOMAS E. FUJA, MEMBER, IEEE AND CHRIS D. HEEGARD, MEMBER, IEEE

Abstract—**Consider a channel with inputs and outputs in the field F_q ($q > 2$). We say the channel is skewed on a set $\mathscr{B} \subset F_q^*$ if the additive noise generated by the channel is likely to lie in $\mathscr{B}$; that is, $\mathscr{B}$ is a set of "common" errors. Our concern is the construction of focused codes that are appropriate for such channels. We say a code is (t_1, t_2)-focused on $\mathscr{B}$ if it can correct up to $t_1 + t_2$ errors provided at most t_1 of those errors lie outside of $\mathscr{B}$; the strategy is to offer different levels of protection against "common" and "uncommon" errors and so provide novel trade-offs between performance and rate. Techniques for constructing focused codes and bounds on their rates are described.**

I. Introduction and Motivation

When a symbol from a codeword over F_q is transmitted over a channel with additive noise, there are $q-1$ different noise symbols that can afflict the transmitted field element. "Traditional" error control codes—designed with respect to the Hamming metric—treat each of these $q-1$ possibilities the same, as simply representing a generic "error."

In many data communication and data storage systems there are some errors that are much more common than others. Consider, for instance, a random access memory system that employs "byte-wide" RAM chips; that is, each chip puts out $b \geq 2$ bits at a time. It has been suggested that codes over F_{2^b} be used for such systems, with each chip's output constituting one element of F_{2^b}. Now the vast majority of chip failures are single-cell failures and so would affect only one bit per byte; thus, most of the symbol errors that would confront such a code would be one of the b field elements with exactly one non-zero bit in its binary representation. Of course, there are failure mechanism that can cause multiple bit failures—catastrophic whole-chip failures, for instance—so we would need to provide *some* protection against arbitrary errors; however, providing the same degree of protection against common and uncommon errors is not efficient.

As another example, consider a modulation scheme with a signal space with $M = 2^b$ signals; assume that data is mapped onto the signals using a Gray code so that the most likely detection errors cause exactly one bit error. Once again, if a code over F_{2^b} is used in such a system, the vast majority of the symbol errors will consist of exactly one incorrect bit.

The previous two examples illustrate one of the most common applications where it becomes desirable to differentiate between two different kinds of errors—when we wish to correct single-bit errors using a nonbinary code. One of our goals is to extend previous results that have described codes capable of correcting all single-bit errors and detecting all other symbol errors [1], [2]. In this sense our work has much in common with recent research by Piret [3] and Boly and van Gils [4].

Finally, there are some applications for which the set of common errors is not simply the single-bit errors. Consider, for example, space-borne RAM systems organized into b-bit bytes; they are typically afflicted by errors falling into one of two categories: either single-bit errors or two-bits-adjacent errors. In this case our set of common errors would contain $2b-1$ elements.

In these and in many other applications it is desirable to "focus" the capabilities of a code on a class of particularly common errors. In this paper we begin by deriving some simple information theory results for channels exhibiting this kind of "skewed" behavior. Following that, we introduce the notion of a focused code [5], [6], and give a technique for constructing them. Finally, we derive bounds on the rates of such codes for a given blocklength and for asymptotically large blocklength.

II. Shannon Theory for Focused Channels

Consider the following symmetric channel model for storage or transmission. A character $X \in F_q$ is to be transmitted and the character $Y = X + Z \in F_q$ is received. It is assumed that the random error $Z \in F_q$ is independent of the input X, and the probability of error, $Pr(Z \neq 0) = \epsilon$. In a typical model for a symmetric channel, the conditional error probability, $Pr(Z = z | Z \neq 0) = 1/(q-1)$, is uniform over the error values where $z \in F_q^* =$

Manuscript received February 28, 1989; revised December 6, 1989. T. E. Fuja was supported in part by the National Science Foundation Engineering Research Centers Program, NSFD CDR 8803012; and by a grant from the Minta Martin Aeronautical Research Fund. C. D. Heegard was supported in part by National Science Foundation grants ECS83-52220 and MIP87-11793. This work was presented at the 1988 Conference on Information Sciences and Systems, March 16–18, 1988, Princeton, NJ; also at the 1988 Allerton Conference on Communications, Control, and Computers, September 27–30, 1988, Monticello, IL.

T. E. Fuja is with the Department of Electrical Engineering, Systems Research Center, University of Maryland, 2219 AV Williams Bldg., College Park, MD 20742.

C. D. Heegard is with the School of Electrical Engineering, Phillips Hall, Cornell University, Ithaca, NY 14853.

IEEE Log Number 9034934.

0018-9448/90/0700-0773$01.00 ©1990 IEEE

$F_q - \{0\}$. We say that a channel is *skewed on a subset* $\mathscr{B} \subset F_q^*$ if $Pr(Z \in \mathscr{B} | Z \neq 0) > |\mathscr{B}|/(q-1)$. In particular, we consider the following distribution for the skewed error Z

$$Pr(Z = z) = \begin{cases} 1-\epsilon, & \text{if } z = 0; \\ \epsilon(1-\gamma)/|\mathscr{B}|, & \text{if } z \in \mathscr{B}; \\ \epsilon\gamma/|\mathscr{B}^c|, & \text{if } z \in \mathscr{B}^c \end{cases}$$

where $\mathscr{B}^c \triangleq F_q^* - \mathscr{B}$. Here, ϵ is the probability of error, and γ is the probability that an error lies outside the set $\mathscr{B}$, given that an error has occurred. Typically we assume that ϵ and γ are both very small; thus, the elements of $\mathscr{B}$ constitute the "common" errors and the elements of $\mathscr{B}^c$ are the "uncommon" errors. Within each class of errors, we assume a uniform distribution.

We call such an error model the *skewed symmetric channel* (SSC) for the common error set $\mathscr{B} \subset F_q^*$. Note that the cases of interest have parameters $0 \leq \epsilon \leq (q-1)/q$ and $0 \leq \gamma \leq |\mathscr{B}^c|/(q-1)$. We are interested in finding the Shannon capacity of this channel as a tool in understanding the problem of constructing focused codes.

Theorem 1: The capacity of the SSC for the common error set $\mathscr{B} \subset F_q^*$ is given by

$$C = 1 - \left[h(\epsilon) + \epsilon\big(h(\gamma) + (1-\gamma)\log_q|\mathscr{B}| + \gamma\log_q|\mathscr{B}^c|\big)\right]$$

where

$$h(x) \triangleq -x\log_q(x) - (1-x)\log_q(1-x)$$

is the *binary entropy function.*

Proof: As we know [7]–[9], the capacity is given by

$$C = \max_{p(x)} I(X;Y)$$

where $I(X;Y)$ is the mutual information between the input X and the output Y and $p(x)$ is a probability distribution on X. In this case, $I(X;Y) = H(Y) - H(Z) \leq 1 - H(Z)$ with equality if the input distribution, $p(x) = 1/q$, is uniform. Finally, to compute $H(Z)$ we note that if we define

$$W \triangleq \begin{cases} 0, & \text{if } Z = 0; \\ 1, & \text{if } Z \in \mathscr{B}; \\ 2, & \text{if } Z \in \mathscr{B}^c \end{cases}$$

then $H(Z) = H(Z,W) = H(W) + H(Z|W)$ and $H(W) = h(\epsilon) + \epsilon h(\gamma)$, $H(Z|W) = \epsilon(1-\gamma)\log_q|\mathscr{B}| + \epsilon\gamma\log_q|\mathscr{B}^c|$. This shows the result. □

In Fig. 1 we have graphed the capacity of the skewed symmetric channel over F_{256} when $|\mathscr{B}| = 8$; this corresponds to the case when data is stored or transmitted in 8-bit bytes and the most common errors are those affecting exactly one bit per byte. We have graphed the capacity for values of the crossover probability ϵ from 10^{-1} to 10^{-3}. In addition, we have varied the values of γ—the probability of an uncommon error given that an error has occurred—from 0 (corresponding to a channel in which only one-bit-per-byte errors can occur) to 247/255, which corresponds to a channel where all errors are equally likely—that is, an "unskewed" channel.

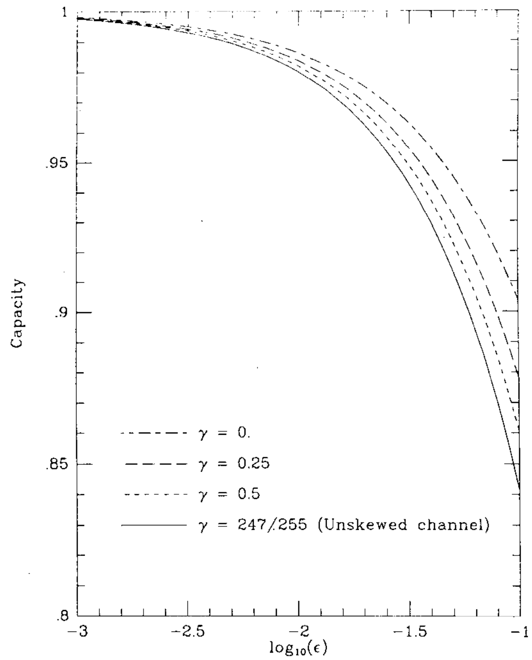

Fig. 1. Capacity of skewed symmetric channel over F_{256} when $|\mathscr{B}| = 8$.

A question related to capacity will help in the description of asymptotic bounds on the performance of focused codes. Given bounds $0 \leq \epsilon \leq \epsilon_0$, $0 \leq \gamma \leq \gamma_0$ what is the maximum value for the entropy of the error $H(Z)$? The following two lemmas provide the answer.

Lemma 1: Let $0 \leq \gamma \leq \gamma_0$ and define

$$\Gamma(\gamma) \triangleq h(\gamma) + (1-\gamma)\log_q|\mathscr{B}| + \gamma\log_q|\mathscr{B}^c|$$

then $\Gamma(\gamma)$ is maximum for

$$\gamma = \min\left\{\gamma_0, \frac{|\mathscr{B}^c|}{(q-1)}\right\}.$$

Proof: To achieve the inequality $d\Gamma/d\gamma \geq 0$ requires

$$\frac{d\Gamma}{d\gamma} = \log_q\left(\frac{1-\gamma}{\gamma}\right) - \log_q|\mathscr{B}| + \log_q|\mathscr{B}^c| \geq 0$$

or $\gamma \leq |\mathscr{B}^c|/(q-1)$. □

Note that $\log_q|\mathscr{B}| \leq \Gamma(\gamma) \leq \log_q(q-1)$.

Lemma 2: Let $0 \leq \epsilon \leq \epsilon_0$, and define

$$f(\epsilon) \triangleq h(\epsilon) + \epsilon\Gamma$$

where $\log_q|\mathscr{B}| \leq \Gamma \leq \log_q(q-1)$. Then $f(\epsilon)$ is maximum for

$$\epsilon = \min\left\{\epsilon_0, \frac{q^\Gamma}{1+q^\Gamma}\right\}.$$

Proof: To achieve the inequality $df/d\epsilon \geq 0$ requires

$$\frac{df}{d\epsilon} = \log_q\left(\frac{1-\epsilon}{\epsilon}\right) + \Gamma \geq 0$$

or $\epsilon \leq q^\Gamma/(1+q^\Gamma)$. □

Theorem 2: For $0 \leq \epsilon \leq \epsilon_0$, $0 \leq \gamma \leq \gamma_0$, the entropy $H(Z)$ is maximized when

$$\gamma = \min\left\{\gamma_0, \frac{|\mathscr{B}^c|}{(q-1)}\right\}, \qquad \epsilon = \min\left\{\epsilon_0, \frac{q^{\Gamma(\gamma)}}{1+q^{\Gamma(\gamma)}}\right\}$$

where

$$\Gamma(\gamma) \triangleq h(\gamma) + (1-\gamma)\log_q|\mathscr{B}| + \gamma\log_q|\mathscr{B}^c|.$$

Proof: Follows immediately from Lemmas 1 and 2. Note that when ϵ and γ are chosen as indicated, then $H(Z) = h(\epsilon) + \epsilon\Gamma(\gamma)$. □

III. Focused Codes—Definitions and a Sufficient Condition for Their Construction

In this section we formulate a class of codes that are appropriate for skewed channels. We call these codes *focused codes*, and they allow us to provide different levels of protection against common and uncommon errors. In Section 3-A we develop the notion of focused codes capable of correcting a specified class of errors; in Section 3-B this is generalized to include simultaneous correction and detection. Finally, in Section 3-C we briefly compare our formulation of focused codes with the codes for simultaneous bit-and-symbol correction described in [3], [4].

A. Focused Codes for Correcting Skewed Errors

For any $\boldsymbol{x} \in F_q^n$ we denote the Hamming weight of $\boldsymbol{x}$ by $\|\boldsymbol{x}\|$; that is, if $\boldsymbol{x} = [x_0, x_1, \cdots, x_{n-1}]$, then

$$\|\boldsymbol{x}\| \triangleq \sum_{i=0}^{n-1} \mathbf{1}_{F_q^*}(x_i)$$

where $\mathbf{1}(\cdot)$ is the indicator function (i.e., $\mathbf{1}_{\mathscr{A}}(x)$ equals one if $x \in \mathscr{A}$ and equals zero otherwise) and F_q^* is the set of nonzero elements of F_q.

More generally, for any set $\mathscr{A} \subseteq F_q^*$ define the $\mathscr{A}$-weight of $\boldsymbol{x} \in F_q^n$ as the number of components of $\boldsymbol{x}$ that lie in $\mathscr{A}$; if we denote the $\mathscr{A}$-weight of $\boldsymbol{x}$ by $\|\boldsymbol{x}\|_{\mathscr{A}}$, then

$$\|\boldsymbol{x}\|_{\mathscr{A}} \triangleq \sum_{i=0}^{n-1} \mathbf{1}_{\mathscr{A}}(x_i).$$

Definition: Let $\mathscr{B} \subset F_q^*$ be a set of non-zero elements of F_q. A code that is (t_1, t_2)-focused on $\mathscr{B}$ is a code that is capable of correcting up to $t_1 + t_2$ errors provided at most t_1 of those errors lie outside $\mathscr{B}$. More precisely, such a code is a set $\mathscr{C}$ of n-tuples over F_q with the following decoding property. There exists a decoding function f: $F_q^n \rightarrow \mathscr{C}$ such that $f(\boldsymbol{c} + \boldsymbol{e}) = \boldsymbol{c}$ for any $\boldsymbol{c} \in \mathscr{C}$ and any $\boldsymbol{e} \in F_q^n$ satisfying the following two conditions:

1) $\|\boldsymbol{e}\| \leq t_1 + t_2$;
2) $\|\boldsymbol{e}\|_{\mathscr{B}^c} \leq t_1$.

Note that a code that is $(t,0)$-focused is a "traditional" t-error correcting code. On the other hand, a $(0,t)$-focused code is guaranteed only to correct errors in the common error set $\mathscr{B}$.

The following lemma gives sufficient conditions for a set of q-ary n-tuples to form a code that is focused on the common set of errors $\mathscr{B} \subset F_q^*$.

Lemma 3: Let $\mathscr{C}$ be a set of q-ary n-tuples with the following property. For any $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathscr{C}$, at least one of the following conditions holds:

1) $\|\boldsymbol{c}_1 - \boldsymbol{c}_2\| > 2t_1 + 2t_2$;
2) $\|\boldsymbol{c}_1 - \boldsymbol{c}_2\| + \|\boldsymbol{c}_1 - \boldsymbol{c}_2\|_{\mathscr{B}^c} > 4t_1 + 2t_2$.

Then $\mathscr{C}$ is (t_1, t_2)-focused on $\mathscr{B}$.

Proof: Let $\mathscr{E}_n \triangleq \{\boldsymbol{x} \in F_q^n: \|\boldsymbol{x}\| \leq t_1 + t_2, \|\boldsymbol{x}\|_{\mathscr{B}^c} \leq t_1\}$ denote the set of error patterns we want to correct. Then as long as $\boldsymbol{c}_1 + \boldsymbol{e}_1 \neq \boldsymbol{c}_2 + \boldsymbol{e}_2$ (or equivalently, $\boldsymbol{e}_1 - \boldsymbol{e}_2 \neq \boldsymbol{c}_2 - \boldsymbol{c}_1$) for any codewords $\boldsymbol{c}_1, \boldsymbol{c}_2$ and any $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathscr{E}_n$, the code will be (t_1, t_2)-focused on $\mathscr{B}$. Therefore, as long as all differences between codewords lie outside

$$\Delta\mathscr{E}_n \triangleq \{\boldsymbol{e}_1 - \boldsymbol{e}_2: \boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathscr{E}_n\}$$

the code will be focused. But in fact it is easily seen that $\Delta\mathscr{E}_n \subseteq \mathscr{A}_n$, where

$$\mathscr{A}_n \triangleq \{\boldsymbol{x}: \|\boldsymbol{x}\| \leq 2t_1 + 2t_2, \|\boldsymbol{x}\| + \|\boldsymbol{x}\|_{\mathscr{B}^c} \leq 4t_1 + 2t_2\}.$$

Thus the lemma is proved. □

The implications of this lemma are presented graphically in Fig. 2. We can plot every q-ary n-tuple in two dimensions by its Hamming weight and its $\mathscr{B}^c$-weight. The lemma says that as long as no codeword difference lies in the shaded region, the code will be (t_1, t_2)-focused on $\mathscr{B}$. By comparison, to insure correction of *all* error patterns of Hamming weight $t_1 + t_2$ or less we would require that all codeword differences have Hamming weight greater than $2t_1 + 2t_2$; by lowering our requirements we have cut a "notch" in the "forbidden zone." This suggests that rate improvements are likely.

It's worth noting that the sufficient conditions given in Lemma 3 are not, in general, necessary conditions since $\mathscr{E}_n$ is often a strict subset of $\mathscr{A}_n$. However, they are necessary conditions if and only if every element of $\mathscr{B}^c$

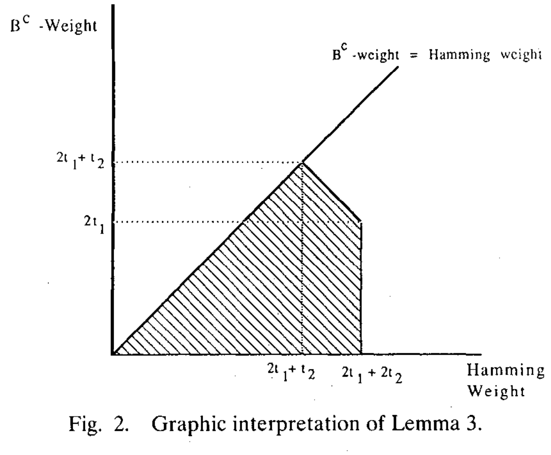

Fig. 2. Graphic interpretation of Lemma 3.

can be expressed as the difference of two elements of $\mathscr{B}$. This means, for instance, that whenever $\mathscr{B}^c$ lies inside a proper additive subgroup of F_q, then the conditions of Lemma 3 are necessary and sufficient; this follows from the fact that every element in an additive group can be expressed as the difference of elements in a coset of that group.

B. Focused Code for Simultaneous Correction and Detection

In this section we briefly show how the definitions and results from the last section can be generalized so as to allow simultaneous correction and detection of a class of skewed errors.

Let $\mathscr{E}_n^c(t_1,t_2)$ denote the set of errors that would be corrected by a code that is (t_1,t_2)-focused on $\mathscr{B}$—i.e., $\mathscr{E}_n^c(t_1,t_2) \triangleq \{x \in F_q^n\colon \|x\| \le t_1+t_2,\ \|x\|_{\mathscr{B}^c} \le t_1\}$. It is obvious that $\mathscr{E}_n^c(t_1,t_2) \subseteq \mathscr{E}_n^c(t_3,t_4)$ if and only if $t_1+t_2 \le t_3+t_4$ and $t_1 \le t_3$.

Definition: For a given n and q, let t_1, t_2, t_3, and t_4 be four integers such that $\mathscr{E}_n^c(t_1,t_2) \subseteq \mathscr{E}_n^c(t_3,t_4)$. Then we say that a code is a (t_1,t_2)-correcting, (t_3,t_4)-detecting focused code if it is capable of correcting any error that lies in $\mathscr{E}_n^c(t_1,t_2)$ and can simultaneously detect any error lying in $\mathscr{E}_n^c(t_3,t_4)$.

We can immediately generalize Lemma 3 to provide the following sufficient condition for the construction of a (t_1,t_2)-correcting, (t_3,t_4)-detecting code; the proof of the generalization is analogous to that of the lemma and is omitted.

Generalization of Lemma 3: Let $\mathscr{C}$ be a set of q-ary n-tuples with the following property. For any $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathscr{C}$, at least one of the following conditions holds:

1) $\|\boldsymbol{c}_1-\boldsymbol{c}_2\| > t_1+t_2+t_3+t_4$;
2) $\|\boldsymbol{c}_1-\boldsymbol{c}_2\|_{\mathscr{B}^c} > t_1+t_3+\min(t_2,t_4)$;
3) $\|\boldsymbol{c}_1-\boldsymbol{c}_2\|+\|\boldsymbol{c}_1-\boldsymbol{c}_2\|_{\mathscr{B}^c} > 2(t_1+t_3)+t_2+t_4$.

Then $\mathscr{C}$ is (t_1,t_2)-focused on $\mathscr{B}$ and furthermore is (t_1,t_2)-correcting, (t_3,t_4)-detecting.

A graphical representation of this generalization is shown in Fig. 3; once again, as long as all codeword differences lie outside the shaded region, the code will have the desired property.

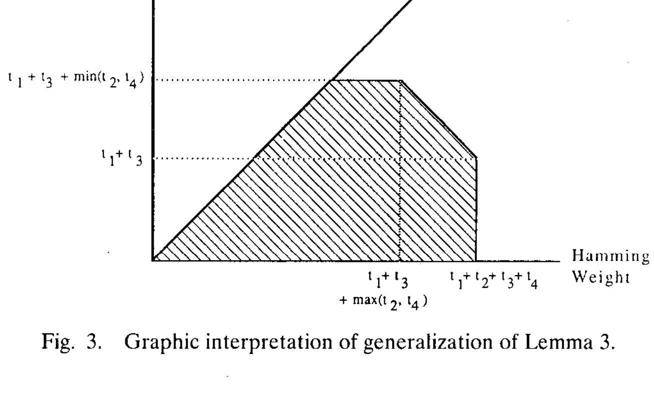

Fig. 3. Graphic interpretation of generalization of Lemma 3.

C. A Comparison with Codes Designed with Respect to the Minimum Distance Profile

In previous papers, Piret [3] and Boly and van Gils [4] considered the problem of simultaneous correction of bit errors and symbol errors. Since this problem was one of the prime motivations for the development of focused codes, we briefly compare the techniques described in [3], [4] with those in this paper.

The formulation of the bit-and-symbol correcting properties discussed in [3]–[4] is as follows. Suppose we wish to form a code over F_{2^b} $(b \ge 2)$ capable of simultaneous bit and symbol correction, that is, we wish to differentiate in some way between correcting symbols (elements of F_{2^b}) and bits (1's and 0's obtained from the binary representation of the elements of F_{2^b}). Let $\mathscr{T} = \{(a_1,b_1),(a_2,b_2),\cdots,(a_{|\mathscr{T}|},b_{|\mathscr{T}|})\}$ be a set of pairs of natural numbers such that $a_i \ne a_j$ for $i \ne j$. Associated with $\mathscr{T}$ is a set $E(\mathscr{T})$ of 2^b-ary n-tuples; $\boldsymbol{x} \in E(\mathscr{T})$ if and only if there exists an $(a_i,b_i) \in \mathscr{T}$ such that by puncturing $\boldsymbol{x}$ in a_i symbol locations one can obtain a vector with at most b_i 1's in its binary representation. Then a code is referred to as $\mathscr{T}$-correcting if it can correct any channel errors lying in $E(\mathscr{T})$.

The difference between the Piret–Boly–van Gils formulation of bit-and-symbol error correcting codes and the formulation embodied by focused codes is due to the intended application of each. The codes of [3]–[4] were constructed for, channels described by the two-state Gilbert model for burst noise—a model for a binary channel. In the Gilbert model errors can occur in "bursts"—occurring when the channel is in the bad state—or they can be "random" errors, occurring when the channel is in the good state. It is assumed that the bits are organized into symbols and that burst errors will be corrected as symbol errors while random errors will be corrected as bit errors; the Piret–Boly–van Gils formulation allows for the fact that it is possible to have two (or more) random errors occurring in a single symbol.

Focused codes, on the other hand, are codes for channels that are intrinsically symbol-organized.

It is easy to show that a code that is (t_1,t_2)-focused on the set of single-bit-per-byte errors can be described (in the parlance of [3]–[4]) as $\mathscr{T}$-correcting, where

$$\begin{aligned}\mathscr{T} = \{&(t_1,\min(t_2,1)),(t_1-1,\min(t_2+1,3)),\\ &(t_1-2,\min(t_2+2,5)),\\ &\cdots,(1,\min(t_1+t_2-1,2t_1-1)),\\ &(0,\min(t_1+t_2,2t_1+1))\}.\end{aligned}$$

However, it's important to keep in mind that a (t_1,t_2)-focused code can correct more error patterns than those indicated by $\mathscr{T}$.

IV. Construction of Combined Linear Focused Codes

In this section we describe a very general technique for constructing focused codes. We begin by describing an obvious method for constructing codes focused on the set of odd-weight errors; we then alter that method to improve the rate, and then generalize the result to include many different common error sets.

A. Codes Focused on Odd-Weight Errors

Suppose we wish to construct a code with blocklength n over F_{2^b} that is (t_1, t_2)-focused on the set of odd-weight symbols; that is, the common error set $\mathscr{B}$ consists of all the elements of F_{2^b} with a binary representation containing an odd number of 1's. (Note that this would include the set of single-bit errors.)

1) The Obvious Technique: A simple way to proceed is with a concatenated coding scheme as follows. Start with a code over $F_{2^{b-1}}$ with minimum distance $2t_1 + t_2 + 1$; then, add an extra bit to each code symbol in every codeword so that every symbol has even parity. To see that the resulting set of n-tuples over F_{2^b} is (t_1, t_2)-focused on the set of odd weight errors, consider the following decoding algorithm. When an n-tuple over F_{2^b} is received at the decoder, the parity of each symbol is checked; where a parity violation occurs, that symbol is marked as an erasure for decoding by the "outer" code with $d_{\min} = 2t_1 + t_2 + 1$. This scheme will correct any combination of $t_1 + t_2$ errors as long as no more than t_1 of those errors have even parity—and thus must be corrected by the outer code without benefit of erasure. This technique constructs codes that have rate $R_2(b-1)/b$, where R_2 is the rate of the outer code.

2) An Improvement to the Obvious Technique: For any n-tuple $\boldsymbol{x}$ over F_{2^b}, let $b(\boldsymbol{x})$ be the binary n-tuple obtained by taking the mod-two sum of each component of $\boldsymbol{x}$; for example, if $\boldsymbol{x} = [0011, 0100, 1011, 1010, 1111]$, then $b(\boldsymbol{x}) = [01100]$. Then the technique described in Section IV-A-1 can be described as follows: Take a codeword from a code over $F_{2^{b-1}}$ and add one bit to each code symbol so that the resulting n-tuple $\boldsymbol{c}$ satisfies $b(\boldsymbol{c}) = \boldsymbol{0}$. This technique is something of an "overkill," since it permits us to flag *every* occurrence of an odd-weight error, and to fulfill the code's "mission" we need only flag up to $t_1 + t_2$ odd-weight errors.

Consider, then, the following construction. Let $\mathscr{C}_1$ be an (n, nR_1) binary code with minimum distance $d_1 = 2t_1 + 2t_2 + 1$; let $\mathscr{C}_2$ be an (n, nR_2) code over F_{2^b-1} with minimum distance $d_2 = 2t_1 + t_2 + 1$. To construct a codeword from our focused code we first take a codeword from $\mathscr{C}_2$ and add one bit to each code symbol such that $\boldsymbol{c}$, the resulting n-tuple over F_{2^b}, satisfies $b(\boldsymbol{c}) \in \mathscr{C}_1$. (Note that there are $|\mathscr{C}_1|$ ways this can be done for a given codeword from $\mathscr{C}_2$.)

We can see that the code thus constructed is (t_1, t_2)-focused on $\mathscr{B}$ by considering the following decoding algorithm. Given a received 2^b-ary n-tuple $\boldsymbol{r}$, compute $b(\boldsymbol{r})$; find the codeword $\boldsymbol{x} \in \mathscr{C}_1$ that is closest to $b(\boldsymbol{r})$. As long as at most $t_1 + t_2$ odd-weight errors have occurred, $\boldsymbol{x}$ will be equal to $b(\boldsymbol{c})$, where $\boldsymbol{c}$ is the codeword that was actually transmitted. Mark the locations where $\boldsymbol{x}$ differs from $b(\boldsymbol{r})$ as erasures; strip off the last bit in each code symbol and pass the resulting 2^{b-1}-ary n-tuple plus erasure locations to a decoder for $\mathscr{C}_2$. Such a decoder will correct all combinations of $t_1 + t_2$ errors provided at most t_1 of the errors have an even-weight binary representation.

Note that this improved construction technique adds nR_1 information bits to each codeword, when compared with the simpler construction of Section IV-A-1. The overall rate of this code is $R_1 \neq b + R_2(b-1)/b$.

B. A Generalization of the Improved Construction Technique

Here we describe a general technique for constructing a code of blocklength n that is (t_1, t_2)-focused on an arbitrary set $\mathscr{B} \subseteq F_{p^b}^*$. We call the resulting codes *combined linear focused codes*.

Our construction uses three different block codes to form the desired code. The three codes are described as follows.

- $\mathscr{C}_0$ is a (b, k_0) code over F_p capable of detecting any error in $\mathscr{B}$; that is, if we consider $\mathscr{B}$ as a set of b-tuples over F_p, then we want $\mathscr{C}_0$ to be a set of b-tuples over F_p such that $\boldsymbol{c}_0 + \boldsymbol{e} \notin \mathscr{C}_0$ for every $\boldsymbol{c}_0 \in \mathscr{C}_0$ and every $\boldsymbol{e} \in \mathscr{B}$. Furthermore, let
$$H_0 = [P_0 | I_{r_0}]$$
be an r_0 $(= b - k_0) \times b$ systematic parity check matrix for $\mathscr{C}_0$; that is, for any $\boldsymbol{e} \in \mathscr{B}$ and any $\boldsymbol{c} \in \mathscr{C}_0$,
$$(\boldsymbol{c} + \boldsymbol{e}) H_0^T = \boldsymbol{e} H_0^T \neq 0.$$
- $\mathscr{C}_1$ is an (n, nR_1) code over $F_{p^{r_0}}$ with minimum distance $d_1 = 2(t_1 + t_2) + 1$.
- $\mathscr{C}_2$ is an (n, nR_2) code over $F_{p^{k_0}}$ with minimum distance $d_2 = 2t_1 + t_2 + 1$.

We construct a codeword from our focused code as follows. Let
$$\boldsymbol{x}[x_0, x_1, \cdots, x_{n-1}] \in \mathscr{C}_1$$
and
$$\boldsymbol{y}[y_0, y_1, \cdots, y_{n-1}] \in \mathscr{C}_2$$
be codewords from $\mathscr{C}_1$ and $\mathscr{C}_2$. Note that each x_i and y_i are elements of $F_{p^{r_0}}$ and $F_{p^{k_0}}$, respectively; thus, each x_i has a unique representation as an r_0-tuple over F_p, and each y_i has a unique representation as a k_0-tuple over F_p. Let $[x_{i,0}, x_{i,1}, \cdots, x_{i,r_0-1}]$ represent x_i and $[y_{i,0}, y_{i,1}, \cdots, y_{i,k_0-1}]$ represent y_i. Furthermore, denote the concatenation of these two strings by (y_i, x_i)—i.e.,
$$(y_i, x_i) \triangleq [y_{i,0}, \cdots, y_{i,k_0-1}, x_{i,0}, \cdots, x_{i,r_0-1}] \in F_p^b.$$
Then the focused codeword $\boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}]$ associated with $\boldsymbol{x}$ and $\boldsymbol{y}$ is obtained by setting
$$c_i = \left(y_i, -(y_i, x_i) H_0^T\right).$$
That is, each symbol in the codeword is represented as a b-tuple over F_p; the first k_0 p-ary digits in each symbol form the corresponding code symbol from $\boldsymbol{y}$. The last r_0 p-ary digits in each symbol come from multiplying the

concatenation of the corresponding symbols from $\boldsymbol{x}$ and $\boldsymbol{y}$ by $-H_0^T$.

We claim that the code consisting of all codewords thus constructed is (t_1,t_2)-focused on $\mathscr{B}$. This is proved by providing a decoding algorithm for the code.

The key point to understanding the algorithm is to recognize that

$$-(y_i, -(y_i,x_i)H_0^T)H_0^T = x_i.$$

Thus, if no error afflicts a code symbol, we can recover the corresponding code symbols from $\boldsymbol{y}$ and $\boldsymbol{x}$. (It's worth nothing that if H_0 is not of the form $[P_0|I_{r_0}]$ then the previous equality does not hold. More generally, if H_0 contains an embedded identity matrix, then it is possible to concatenate the symbols in such a way that both x_i and y_i can be recovered by multiplication by H_0^T.)

The decoding algorithm is as follows. Assume the code vector $\boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}]$ is transmitted, where $c_i = (y_i, -(y_i,x_i)H_0^T)$. Suppose you receive the vector

$$\boldsymbol{r} = [r_0, r_1, \cdots, r_{n-1}] \in F_{p^b}^n.$$

As before, we assume that r_i is represented by the b-tuple $[r_{i,0}, \cdots, r_{i,b-1}]$, $r_{i,j} \in F_p$. For each i, $0 \le i \le n-1$, compute

$$d_i = -[r_{i,0}, \cdots, r_{i,b-1}]H_0^T.$$

If no error occurred in the ith symbol, then, as previously noted, $d_i = x_i$. If, however, the channel imposed a "common" error in the ith symbol (i.e., $r_i = c_i + e$, where $e \in \mathscr{B}$ is an error in our common error set) then $d_i \ne x_i$. Thus, each occurrence of a common error (or any error e for which $eH_0^T \ne 0$) will cause the vector $\boldsymbol{d} = [d_0, d_1, \cdots, d_{n-1}]$ to differ from $\boldsymbol{x}$ in another coordinate. Now provided that no more than $t_1 + t_2$ such errors occur, we can use $\mathscr{C}_1$ to recover $\boldsymbol{x}$ from $\boldsymbol{d}$. Furthermore, we can then use the location of the common errors, which will be indicated by the coordinates where $\boldsymbol{d}$ differed from $\boldsymbol{x}$, as erasures to be used by $\mathscr{C}_2$; in this way, $\boldsymbol{y}$ can be recovered and the decoding process is complete. As long as no more than $t_1 + t_2$ errors occur, and no more than that t_1 lie outside $\mathscr{B}$—and thus have to be corrected without benefit of an erasure—this algorithm will decode correctly.

Finally, the rate of the focused code can be easily computed from the rates of the three constituent codes. If we define R_0, R_1, and R_2 to be the rates of $\mathscr{C}_0$, $\mathscr{C}_1$, and $\mathscr{C}_2$, then the rate R of the focused code is given by

$$R = (1-R_0)R_1 + R_0R_2.$$

Example 1: Let the field be F_{2^b} and let the common error set consist of all odd-weight errors. Then

$$H_0 = (1 \quad 1 \quad 1 \quad \cdots \quad 1),$$

and to compute $\boldsymbol{d}$ you need only take the mod-two sum of the binary representation of each received symbol. Since H_0 is a $1 \times b$ matrix, the "inner code" $\mathscr{C}_1$ is a binary code and the "outer code" $\mathscr{C}_2$ is a code over $F_{2^{b-1}}$. (This is the construction technique described in Section IV-A-2.)

Example 2: Once again let the field be all binary b-tuples, but this time let the common error set be all double errors that are adjacent to one another. In this case, the matrix H_0 is given by $H_0 = (1\ 0\ 1\ \cdots\ 1\ 0)$ (for even b) or $H_0 = (1\ 0\ 1\ \cdots\ 0\ 1)$ (for odd b). Once again, $\mathscr{C}_1$ is a binary code and $\mathscr{C}_2$ is over $F_{2^{b-1}}$.

Example 3: This time, suppose we are interested in *both* odd-weight errors *and* double-adjacent errors. In this case, H_0 is given by

$$H_0 = \begin{pmatrix} 1 & 0 & 1 & 0 & \cdots & 1 & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 1 \end{pmatrix}$$

for even b, or

$$H_0 = \begin{pmatrix} 0 & 1 & 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

for odd b, In this case, $\mathscr{C}_1$ is a code over F_4 and $\mathscr{C}_2$ is over $F_{2^{b-2}}$.

C. Some Numerical Results for Combined Linear Focused Codes

In Fig. 4 we have graphed the rates of two focused codes for blocklengths between 10 and 100. In each case we are assuming that the codes are over F_{256}—thus corresponding to a communication/storage system with 8-bit bytes—and the focus set consists of those field elements with an odd-weight binary representation. (And so $|\mathscr{B}| = 128$.)

The two focused codes we have considered are combined focused codes, constructed using the technique described in Section IV-A-2 (and generalized in Section IV-B). Specifically, we consider a (1,1)-focused code and

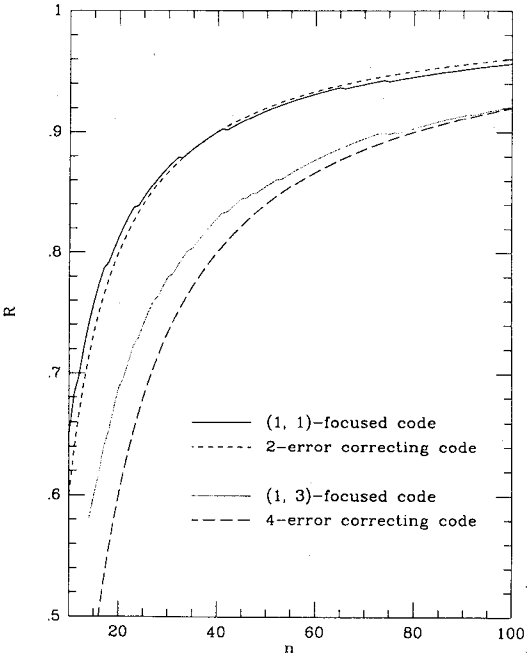

Fig. 4. Rates of (t_1,t_2)-focused codes and $t_1 + t_2$-error correcting Reed–Solomon codes for $(t_1 = 1, t_2 = 1)$ and $(t_1 = 1, t_2 = 3)$.

a (1,3)-focused code; we assume that the outer code in each case is a Reed–Solomon code over F_{128} with minimum distance $2t_1+t_2+1$. The rate of the inner code–the binary code with minimum distance $d_{\min}=2(t_1+t_2)+1$—was determined from a table of "good" codes [10]. For comparison's sake we have included a graph of the rates for a t_1+t_2-error correcting Reed–Solomon code over F_{256} so that it can be seen what is gained by failing to correcting the uncommon errors of Hamming weight t_1+t_2.

It is seen that the gains are modest for the (1,1)-code; for $n=10$ there is a rate improvement of only 8.3%, and as the blocklength increases that improvement vanishes, with the Reed–Solomon code actually having a higher rate when $n \ge 41$. For the (1,3)-focused code, the improvement is more impressive; for $n=14$ there is a 35% improvement in the rate (from 0.43 from the Reed–Solomon code to 0.58 for the focused code), and over the entire range of n the focused code has a higher rate than the Reed–Solomon code. (Although the improvement is insignificant for large n and would once again go negative if we took n much bigger than 100.)

These results reinforce the common-sense idea that the more "focused" a code is—that is, the more error patterns we avoid correcting—the bigger the payoff in terms of rate. This notion is expressed quantitatively in terms of asymptotic rate bounds at the end of Section V-B.

V. Bounds for Focused Codes

In this section we compute bounds on the rates of arbitrary focused codes for fixed blocklength and for asymptotically large blocklength. We also compute asymptotic bounds on the rates of the combined focused codes of Section IV-B.

A. Bounds for Focused Codes of Fixed Blocklength

The rate R of a code $\mathcal{C}$ over F_q is defined as $R \triangleq (1/n)\log_q|\mathcal{C}|$. For a given blocklength n, nonnegative integers t_1 and t_2, field F_q, and common error set $\mathcal{B}$, we let $R_n^*(t_1,t_2)$ denote the highest rate of any code of blocklength n over F_q that is (t_1,t_2)-focused on $\mathcal{B}$;

$$R_n^*(t_1,t_2) \triangleq \sup\{R\text{: There exists a code of rate } R \text{ and blocklength } n \text{ that is } (t_1,t_2)\text{—focused on } \mathcal{B}\}.$$

Theorem 3: $R_n^*(t_1,t_2) \le 1-(1/n)\log_q(|\mathcal{E}_n|)$, where

$$|\mathcal{E}_n| = \sum_{i=0}^{t_1+t_2}\sum_{j=0}^{\min(i,t_1)}\binom{n}{i}\binom{i}{j}|\mathcal{B}|^{i-j}|\mathcal{B}^c|^j.$$

Proof: Let $\mathcal{E}_n \triangleq \{x \in F_q^n\colon \|\boldsymbol{x}\| \le t_1+t_2,\ \|\boldsymbol{x}\|_{\mathcal{B}^c} \le t_1\}$ be the set of error patterns we want to correct. Let $\mathcal{C}$ be any code that is (t_1,t_2)-focused on $\mathcal{B}$. For every codeword $\boldsymbol{c} \in \mathcal{C}$ there is a region about $\boldsymbol{c}$ containing the $|\mathcal{E}_n|$ n-tuples over F_q that would be mapped onto $\boldsymbol{c}$ by a decoder for $\mathcal{C}$. Clearly, the volume of all these regions summed over the whole code cannot be greater than q^n; this gives us the bound

$$|\mathcal{C}| \le q^n/|\mathcal{E}_n|,$$

which is equivalent to the theorem. □

To provide a lower bound on $R_n^*(t_1,t_2)$, we recall some notation from Lemma 3; let $\Delta\mathcal{E}_n$ be the set of differences of correctable errors i.e.,

$$\Delta\mathcal{E}_n = \{\boldsymbol{e}_1-\boldsymbol{e}_2\colon \boldsymbol{e}_1,\boldsymbol{e}_2 \in \mathcal{E}_n\}.$$

Theorem 4: For any positive integers n and M satisfying

$$(M-1)\cdot|\Delta\mathcal{E}_n| < q^n$$

there exists a code of blocklength n over F_q that has M codewords and is (t_1,t_2)-focused on $\mathcal{B}$.

Proof: The proof is by induction on M; it's trivially true for $M=1$.

So, assume there exists a (t_1,t_2)-focused code with $M-1$ codewords; call this code $\mathcal{C}_{M-1}$. Furthermore, for any q-ary n-tuple $\boldsymbol{c}$ let $\boldsymbol{c}+\Delta\mathcal{E}_n$ consist of the set obtained when each element of $\Delta\mathcal{E}_n$ is added to $\boldsymbol{c}$; that is,

$$\boldsymbol{c}+\Delta\mathcal{E}_n \triangleq \{\boldsymbol{c}+\Delta\boldsymbol{e}\colon \Delta\boldsymbol{e} \in \Delta\mathcal{E}_n\}.$$

Then from the union bound

$$\left|\bigcup_{\boldsymbol{c}\in\mathcal{C}_{M-1}} \boldsymbol{c}+\Delta\mathcal{E}_n\right| \le (M-1)\cdot|\Delta\mathcal{E}_n|$$

and so by the induction hypothesis

$$\left|\bigcup_{\boldsymbol{c}\in\mathcal{C}_{M-1}} \boldsymbol{c}+\Delta\mathcal{E}_n\right| < q^n.$$

This means that there exists $\boldsymbol{x} \in F_q^n$ such that

$$\boldsymbol{x} \notin \bigcup_{\boldsymbol{c}\in\mathcal{C}_{M-1}} \boldsymbol{c}+\Delta\mathcal{E}_n.$$

By definition of $\Delta\mathcal{E}_n$, then, for any $\boldsymbol{c} \in \mathcal{C}_{M-1}$ and any correctable error pattern $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$,

$$\boldsymbol{c}+\boldsymbol{e}_1 \ne \boldsymbol{x}+\boldsymbol{e}_2.$$

And so

$$\mathcal{C}_M = \mathcal{C}_{M-1} \cup \{\boldsymbol{x}\}$$

is a (t_1,t_2)-focused code with M codewords. □

Corollary to Theorem 4: $R_n^*(t_1,t_2) \ge 1-(1/n)\log_q(|\mathcal{A}_n|)$, where

$$|\mathcal{A}_n| = \sum_{i=0}^{2t_1+2t_2}\sum_{j=0}^{\min(i,4t_1+2t_2-i)}\binom{n}{i}\binom{i}{j}|\mathcal{B}|^{i-j}|\mathcal{B}^c|^j.$$

Proof: Theorem 4 implies that such a code exists if

$$R < 1-\frac{1}{n}\log_q(|\Delta\mathcal{E}_n|).$$

By noting that $\Delta\mathcal{E}_n \subseteq \mathcal{A}_n$, where

$$\mathcal{A}_n \triangleq \{\boldsymbol{x} \in F_q^n\colon \|\boldsymbol{x}\| \le 2t_1+2t_2,\ \|x\|+\|\boldsymbol{x}\|_{\mathcal{B}^c} \le 4t_1+2t_2\}$$

the corollary follows. □

Note that Theorem 3 is an inequality in the form of a "sphere packing" or Hamming bound; Theorem 4 is similar to the Gilbert–Varshamov bound.

Finally, it should be noted that if we assume that the field we are working over has characteristic two (i.e., $q=2^b$ for some b) then the previous theorem can be modified to guarantee the existence of codes that form an additive group.

Theorem 5: For any $q=2^b$ and any integers n and j satisfying

$$2^{j-1}|\Delta\mathscr{C}_n| < q^n$$

there exists a (t_1,t_2)-focused code of blocklength n over F_q that has 2^j codewords and that forms an additive subgroup of F_q^n.

Proof: The proof is very similar to that of the previous theorem but using induction on j instead. The theorem is obviously true for $j=1$, since $|\Delta\mathscr{C}_n| < q^n$ implies the existence of an n-tuple $\boldsymbol{c} \notin \Delta\mathscr{C}_n$, and the code

$$\mathscr{C}_2 \triangleq \{\boldsymbol{0},\boldsymbol{c}\}$$

is a (t_1,t_2)-focused code with two codewords.

If we then assume by the induction hypothesis that there exists a group code $\mathscr{C}_{2^{j-1}}$ with 2^{j-1} codewords, then the inequality $2^{j-1}|\Delta\mathscr{C}_n| < q^n$ means that there exists a vector $\boldsymbol{x}$ that is not in $\boldsymbol{c}+\Delta\mathscr{C}_n$ for any $\boldsymbol{c}\in\mathscr{C}_{2^{j-1}}$. Define $\mathscr{C}_{2^j}$ to be the union of $\mathscr{C}_{2^{j-1}}$ and the coset of $\mathscr{C}_{2^{j-1}}$ that contains $\boldsymbol{x}$, i.e.,

$$\mathscr{C}_{2^j} = \mathscr{C}_{2^{j-1}} \bigcup (\boldsymbol{x}+\mathscr{C}_{2^{j-1}}).$$

If F_q has characteristic two, then $\mathscr{C}_{2^j}$ is an additive group with 2^j elements. (The requirement that $q=2^b$ is necessary to ensure that $\boldsymbol{x}_1+\boldsymbol{x}_2\in\mathscr{C}_{2^j}$ for $\boldsymbol{x}_1,\boldsymbol{x}_2\in\boldsymbol{x}+\mathscr{C}_{2^{j-1}}$.) It is easily seen that $\boldsymbol{c}_1+\boldsymbol{e}_1\neq\boldsymbol{c}_2+\boldsymbol{e}_2$ for any $\boldsymbol{e}_1,\boldsymbol{e}_2\in\mathscr{E}_n$ and any $\boldsymbol{c}_1,\boldsymbol{c}_2\in\mathscr{C}_{2^j}$ for $\mathscr{C}_{2^j}$ so defined. □

Finally, we can generalize the upper bound of Theorem 4 to include the possibility of simultaneous error correction and detection. Using the definitions from Section III-B, the following theorem gives bounds on the best possible rate that can be achieved by a (t_1,t_2)-correcting, (t_3,t_4)-detecting focused code; the proof is analogous to that of Theorem 4.

Theorem 6: There exists a (t_1,t_2)-correcting, (t_3,t_4)-detecting focused code with rate $R\geq 1-(1/\mathrm{n})\log_q(|\mathscr{D}_n|)$, where

$$|\mathscr{D}_n| = \sum_{\substack{i=0}}^{\substack{t_1+t_2\\+t_3+t_4}} \;\sum_{j=0}^{\substack{\min(i,t_1+t_3\;+\min(t_2,t_4),\\ 2(t_1+t_3)+t_2+t_4-i)}} \binom{n}{i}\binom{i}{j}|\mathscr{B}|^{i-j}|\mathscr{B}^c|^j.$$

B. Asymptotic Bounds for Focused Codes

In this section we are interested in the attainable rates for codes with very long blocklengths. The results from the last section are combined with the results on entropy maximization from Section II to obtain bounds on the asymptotic performance of focused codes. To this end, define

$$R^*(\alpha,\beta) \triangleq \overline{\lim_{n\to\infty}}\, R_n^*(\alpha n,\beta n).$$

Then the following two theorems provide "focused" versions of the asymptotic Gilbert–Varshamov and Hamming bounds.

Theorem 7: $R^*(\alpha,\beta)\geq 1-h(\epsilon)-\epsilon\Gamma(\gamma)$ where

$$\Gamma(\gamma)\triangleq h(\gamma)+(1-\gamma)\log_q|\mathscr{B}|+\gamma\log_q|\mathscr{B}^c|$$

and

$$\epsilon=\min\left\{2\alpha+2\beta,\frac{q^{\Gamma(\gamma)}}{1+q^{\Gamma(\gamma)}}\right\},$$

$$\gamma=\min\left\{\frac{4\alpha+2\beta-\epsilon}{\epsilon},\frac{|\mathscr{B}^c|}{(q-1)}\right\}.$$

Proof:

$$|\mathscr{A}_n| = \sum_{i=0}^{2(\alpha+\beta)n}\;\sum_{j=0}^{\min(i,(4\alpha+2\beta-i)n)}\binom{n}{i}\binom{i}{j}(|\mathscr{B}^c|)^j|\mathscr{B}|^{i-j}$$

$$\leq K\max\left\{\binom{n}{i}\binom{i}{j}(|\mathscr{B}^c|)^j|\mathscr{B}|^{i-j}\colon 0\leq i\leq 2(\alpha+\beta)n,\right.$$

$$\left. 0\leq j\leq\min(i,(4\alpha+2\beta-i)n)\right\}$$

$$\leq K\max\{q^{nE(i,j)}\colon\quad 0\leq i\leq 2(\alpha+\beta)n,\quad 0\leq j\leq\min(i,(4\alpha+2\beta-i)n)\}$$

where

$$E(i,j)=h\left(\frac{i}{n}\right)+\frac{i}{n}h\left(\frac{j}{i}\right)+\frac{j}{n}\log_q|\mathscr{B}^c|+\frac{i-j}{n}\log_q|\mathscr{B}|$$

and K is equal to the number of terms in the double sum. Note that to achieve the last inequality we have made use of the well-known bound [11]

$$\binom{n}{i}\leq q^{n[h(i/n)]}.$$

Note also that K is a polynomial in n and so

$$\lim_{n\to\infty}\frac{1}{n}\log_q(K)=0.$$

The maximum is found by maximizing the exponent

$$h(\epsilon)+\epsilon h(\gamma)+\epsilon\gamma\log_q|\mathscr{B}^c|+\epsilon(1-\gamma)\log_q|\mathscr{B}|$$

where $\epsilon=i/n$ and $\gamma=j/i$. The values of ϵ and γ that maximize the exponent are given in the theorem and follow from Theorem 2. □

Theorem 8:

$$R^*(\alpha,\beta)\leq 1-h(\epsilon)-\epsilon\Gamma(\gamma)$$

where

$$\Gamma(\gamma)\triangleq h(\gamma)+(1-\gamma)\log_q|\mathscr{B}|+\gamma\log_q|\mathscr{B}^c|$$

and

$$\epsilon = \min\left\{\alpha + \beta, \frac{q^{\Gamma(\gamma)}}{1 + q^{\Gamma(\gamma)}}\right\}$$

$$\gamma = \min\left\{\frac{\alpha}{\epsilon}, \frac{|\mathscr{B}^c|}{(q-1)}\right\}.$$

Proof:

$$|\mathscr{E}_n| = \sum_{i=0}^{(\alpha+\beta)n} \sum_{j=0}^{\min(i,\alpha n)} \binom{n}{i}\binom{i}{j}(|\mathscr{B}^c|)^j |\mathscr{B}|^{i-j}$$

$$\geq \max\left\{\binom{n}{i}\binom{i}{j}(|\mathscr{B}^c|)^j|\mathscr{B}|^{i-j}: \quad 0 \leq i \leq (\alpha+\beta)n, 0 \leq j \leq \min(i,\alpha n)\right\}$$

$$\geq \max\{q^{nE(i,j)}: 0 \leq i \leq (\alpha+\beta)n, 0 \leq j \leq \min(i,\alpha n)\}$$

where

$$E(i,j) \triangleq h\left(\frac{i}{n}\right) + \frac{i}{n}h\left(\frac{j}{i}\right) + \frac{j}{n}\log_q|\mathscr{B}^c| + \frac{i-j}{n}\log_q|\mathscr{B}| + o_n$$

and o_n goes to 0 as $n \to \infty$. The last inequality follows from the bound [11]

$$\binom{n}{i} \geq q^{n[h(i/n)+o_n]}.$$

The maximum is found by maximizing the exponent

$$h(\epsilon) + \epsilon h(\gamma) + \epsilon\gamma \log_q|\mathscr{B}^c| + \epsilon(1-\gamma)\log_q|\mathscr{B}|$$

where $\epsilon = i/n$, $\gamma = j/i$. The values of ϵ and γ that maximize the exponent are given in the theorem and again follow from Theorem 2. □

It is interesting to note that when $|\mathscr{B}^c|/(q-1) \leq \alpha/(\alpha + \beta)$ then Theorems 7 and 8 simplify to the "traditional" asymptotic Hamming bound and Gilbert–Varshamov bound for codes capable of correcting a fraction $\alpha + \beta$ of errors in each codeword; this is reasonable, because when this inequality holds then all but a vanishingly small fraction of the errors of Hamming weight $(\alpha+\beta)n$ have $\mathscr{B}^c$-weight less than or equal to αn and would thus be corrected by a $(\alpha n, \beta n)$-focused code.

C. Bounds for Combined Linear Focused Codes

In Section III-B we described a technique for constructing focused codes with block length n over F_{p^b} by combining three different codes in a specific way. In this section we compute bounds on the rates that can be achieved using this technique for asymptotically large n.

Using this technique, we note that the choice of the common error set $\mathscr{B}$ determines the code $\mathscr{C}_0$ as well as the fields over which $\mathscr{C}_1$ and $\mathscr{C}_2$ are formed; $\mathscr{C}_0$ is a $(b, k_0 = b - r_0)$ code over F_p capable of detecting any error in $\mathscr{B}$, $\mathscr{C}_1$ is a code over F_{q_1} $(q_1 = p^{r_0})$ with blocklength n and minimum distance $d_1 = 2t_1 + 2t_2 + 1$, and $\mathscr{C}_2$ is a code over F_{q_2} $(q_2 = p^{k_0})$ with blocklength n and minimum distance $d_1 = 2t_1 + t_2 + 1$. For a given choice of $\mathscr{B}$ (and therefore for a given choice of $\mathscr{C}_0$, which we assume has rate R_0) we can apply the traditional asymptotic rate bounds [11]–[13] to R_1 and R_2 to derive asymptotic bounds for combined linear focused codes. Some of the bounds thus derived are given in Theorem 9.

Theorem 9: Let $\mathscr{B} \subset F_q^*$ $(q = p^b)$ and let

$R_n^c(t_1,t_2) \triangleq \sup\{R$: There exists a combined linear focused code of rate R and blocklength n that is (t_1,t_2)-focused on $\mathscr{B}\}$,

and define

$$R^c(\alpha,\beta) \triangleq \overline{\lim_{n\to\infty}} R_n^c(\alpha n, \beta n).$$

If we define the function $H(\epsilon,m)$ as

$$H(\epsilon,m) \triangleq \frac{h(\epsilon) + \epsilon\log_q(m-1)}{\log_q(m)}$$

the function $G(\epsilon,m)$ as

$$G(\epsilon,m) \triangleq \frac{\epsilon m}{m-1}$$

$\overline{R}_0 \triangleq 1 - R_0$, and $\theta_i \triangleq (q_i - 1)/q_i$ for $i = 1,2$, then the following inequalities hold.

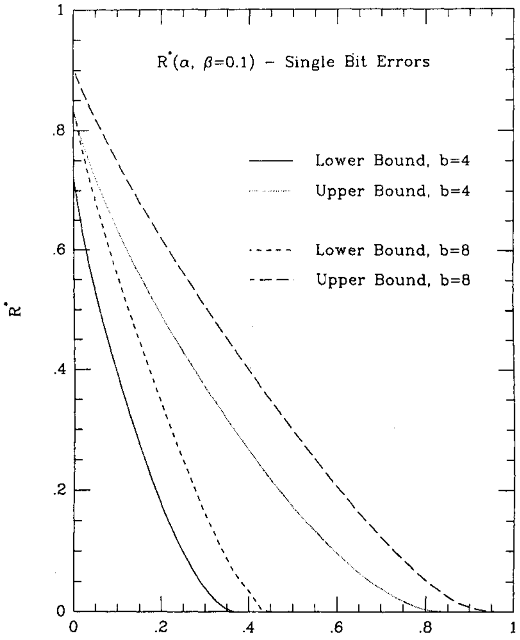

Fig. 5. Upper and lower bonds on $R^*(\alpha, 0.1)$ for codes over F_{16} and F_{256} when $\mathscr{B}$ is set of all field elements with binary representation containing single 1.

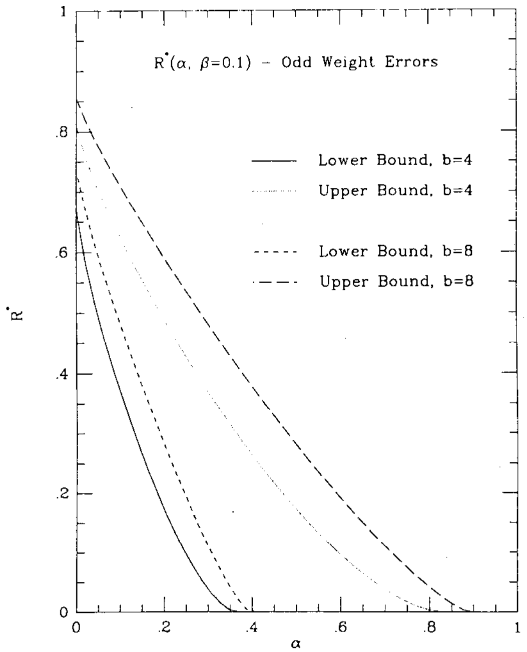

Fig. 6. Upper and lower bounds on $R^*(\alpha,0.1)$ for codes over F_{16} and F_{256} when $\mathscr{B}$ is set of all field elements with binary representation containing odd number of 1's.

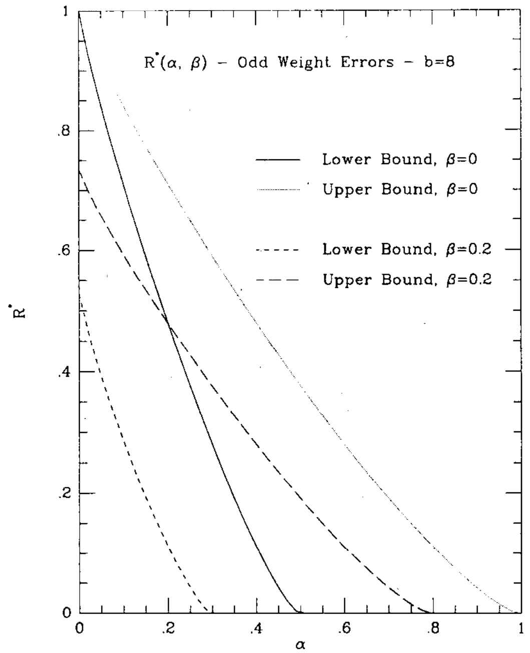

Fig. 7. Upper and lower bounds on $R^*(\alpha,\beta=0,0.2)$ for codes over F_{256} when $\mathscr{B}$ is set of all field elements with binary representation containing odd number of 1's.

Gilbert–Varshamov Bound:

$$R^c(\alpha,\beta)\geq\begin{cases}1-\overline{R}_0H(2\alpha+2\beta,q_1)-R_0H(2\alpha+\beta,q_2), & \text{if } 0\leq 2\alpha+2\beta\leq\theta_1 \text{ and } 0\leq 2\alpha+\beta\leq\theta_2;\\ \overline{R}_0(1-H(2\alpha+2\beta,q_1)), & \text{if } 0\leq 2\alpha+2\beta\leq\theta_1 \text{ and } \theta_2\leq 2\alpha+\beta\leq 1;\\ R_0(1-H(2\alpha+\beta,q_2)), & \text{if } \theta_1\leq 2\alpha+2\beta\leq 1 \text{ and } 0\leq 2\alpha+\beta\leq\theta_2;\\ 0, & \text{if } \theta_1\leq 2\alpha+2\beta\leq 1 \text{ and } \theta_2\leq 2\alpha+\beta\leq 1.\end{cases}$$

Hamming Bound:

$$R^c(\alpha,\beta)\leq\begin{cases}1-\overline{R}_0H(\alpha+\beta,q_1)-R_0H\left(\alpha+\tfrac{1}{2}\beta,q_2\right), & \text{if } 0\leq\alpha+\beta\leq\theta_1 \text{ and } 0\leq\alpha+\tfrac{1}{2}\beta\leq\theta_2;\\ \overline{R}_0(1-H(\alpha+\beta,q_1)), & \text{if } 0\leq\alpha+\beta\leq\theta_1 \text{ and } \theta_2\leq\alpha+\tfrac{1}{2}\beta\leq 1;\\ R_0\left(1-H\left(\alpha+\tfrac{1}{2}\beta,q_2\right)\right), & \text{if } \theta_1\leq\alpha+\beta\leq 1 \text{ and } 0\leq\alpha+\tfrac{1}{2}\beta\leq\theta_2;\\ 0, & \text{if } \theta_1\leq\alpha+\beta\leq 1 \text{ and } \theta_2\leq\alpha+\tfrac{1}{2}\beta\leq 1.\end{cases}$$

Plotkin Bound:

$$R^c(\alpha,\beta)\leq\begin{cases}1-\overline{R}_0G(2\alpha+2\beta,q_1)-R_0G(2\alpha+\beta,q_2), & \text{if } 0\leq 2\alpha+2\beta\leq\theta_1 \text{ and } 0\leq 2\alpha+\beta\leq\theta_2;\\ \overline{R}_0(1-G(2\alpha+2\beta,q_1)), & \text{if } 0\leq 2\alpha+2\beta\leq\theta \text{ and } \theta_2\leq 2\alpha+\beta\leq 1;\\ R_0(1-G(2\alpha+\beta,q_2)), & \text{if } \theta_1\leq 2\alpha+2\beta\leq 1 \text{ and } 0\leq 2\alpha+\beta\leq\theta_2;\\ 0, & \text{if } \theta_1\leq 2\alpha+2\beta\leq 1 \text{ and } \theta_2\leq 2\alpha+\beta\leq 1.\end{cases}$$

D. Numerical Examples of Asymptotic Bounds

Figs. 5–8 shows some of the bounds derived in this section for particular values of q and different focus sets. The following are points of interest.

- A comparison of Figs. 5 and 6 show that relatively little is given up by "focusing" on the odd-weight errors rather than single-bit errors; this is (as is to be expected) especially true when the byte-size is small.
- Fig. 7 demonstrates the observation made at the end of Section V-B. Recalling that a $(t,0)$-focused code is a "traditional" t-error correcting code, this implies that the bounds on $R^*(\alpha,0)$ are the traditional asymptotic Hamming and Gilbert–Varshamov bounds. But it was noted in Section V-B that $R^*(\alpha,\beta)$ is equivalent to this bound when $\alpha/(\alpha+\beta)\geq|\mathscr{B}^c|/(q-1)$. Relating this to Fig. 7, this means that the bounds on $R^*(\alpha,0.2)$ are equivalent to the corresponding bounds on $R^*(\alpha+0.2,0)$ when $\alpha/(\alpha+0.2)\geq 127/255$, or when $\alpha>0.1984$.

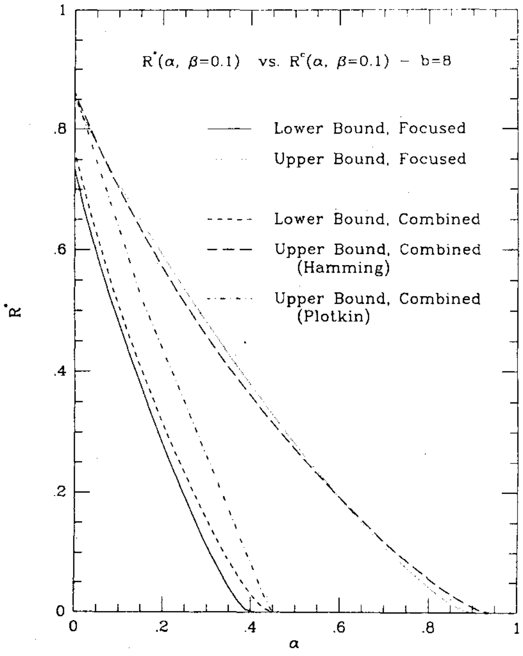

Fig. 8. Upper and lower bounds on asymptotic rates of focused codes and combined linear focused codes. (Focus set is set of all field elements with binary representation containing odd number of 1's.)

- Fig. 8 compares the asymptotic results for focused codes in general with the asymptotic results for combined focused codes derived in Section V-C. It demonstrates the perhaps surprising result that the lower bound on the rates of combined codes can actually exceed that of focused codes in general; a similar phenomenon holds for upper bounds.

VI. Conclusion and Future Work

This paper considered the problem of constructing and analyzing codes that are capable of offering different levels of protection against common and uncommon channel errors. A technique for constructing such codes was described. In addition, bounds on the achievable rates of the codes were derived.

The obvious next question to be answered: What, precisely, are the rate/performance tradeoffs made possible by focused codes? Under what conditions do focused codes offer additional coding gain as compared with error corrrecting codes designed solely with respect to the Hamming metric? These issues are currently being investigated.

References

[1] S. Reddy, "A class of linear codes for error control in byte-per-card organized digital systems," *IEEE Trans. Comput.*, vol. C-27, no. 5, May 1978.

[2] L. Dunning and M. Varanasi, "Code constructions for error control in byte-organized memory systems," *IEEE Trans. Comput.*, vol. C-32, no. 6, June 1983.

[3] P. Piret, "Binary codes for compound channels," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 3, May 1985.

[4] J. P. Boly and W. J. van Gils, "Codes for combined symbol and digit error control," *IEEE Trans. Inform. Theory*, vol. IT-34, no. 5, pp. 1286–1307, Sept. 1988.

[5] T. Fuja and C. Heegard, "Focused error control codes," in *1988 Conf. Inform. Sci. and Syst.*, Princeton Univ., Mar. 16–18, 1988.

[6] ____, "Asymptotic bounds for focused error control codes," in *1988 Allerton Conf. Commun. Control. Comput.*, Monticello, IL, Sept. 27–30, 1988.

[7] R. Gallager, *Information Theory and Reliable Communications.* New York: Wiley, 1968.

[8] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Channels.* New York: Academic, 1981.

[9] Richard Blahut, *Principles and Practice of Information Theory.* New York: Addison-Wesley, 1987.

[10] T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 5, pp. 665–680, Sept. 1989.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North Holland, 1977.

[12] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications.* New York: Prentice-Hall, 1983.

[13] J. H. van Lint, *Introduction to Coding Theory.* New York: Springer-Verlag, 1982.