[8] R. M. Gray, "Time-invariant trellis encoding of ergodic discrete-time sources with a fidelity criterion," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 71–83, Jan. 1977.
[9] A. C. Goris and J. D. Gibson, "Incremental tree coding of speech," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 511–516, July 1981.
[10] A. M. Mood and F. A. Graybill, *Introduction to the Theory of Statistics*, second ed. New York: McGraw-Hill, 1963.
[11] S. Mohan, D. Kryskowski, and C.-M. Lin, "Stack algorithm speech encoding with fixed and variable symbol release rules," *IEEE Trans. Commun.*, vol. COM-33, pp. 1015–1018, Sept. 1985.

Bounds on the Undetected Error Probabilities of Linear Codes for Both Error Correction and Detection

MAO-CHAO LIN

***Abstract*—The $(n, k, d \geq 2t+1)$ binary linear codes are studied, which are used for correcting error patterns of weight at most t and detecting other error patterns over a binary symmetric channel. In particular, for $t=1$, it is shown that there exists one code whose probability of undetected errors is upper bounded by $(n+1)[2^{n-k}-n]^{-1}$ when used on a binary symmetric channel with transition probability less than $2/n$.**

I. Introduction

In pure ARQ systems, linear codes are used solely for detecting errors. Suppose that we apply linear codes to a binary symmetric channel (BSC) with transition probability p. It [1, pp. 78–79] has been proved that for each p with $0 \leq p \leq 1$, there exists an (n, k) binary linear code whose probability of undetected errors (PUDE) is upper bounded by $2^{-(n-k)}$. Hamming codes and double error correcting primitive BCH codes [2], [3] have been proved to satisfy the inequality if the transition probability p is no greater than $1/2$.

Pure ARQ systems have the problem of low throughput if the transition probability in the BSC is high. Therefore, in hybrid ARQ systems [1] especially in type-I hybrid ARQ systems, linear codes are used for correcting some low weight error patterns and detecting many other error patterns. Therefore, it is interesting to study the probability of undetected errors for linear codes that are used for both error correction and error detection over the BSC. In this correspondence, our study is divided into two parts. In the first part, we study the class of $(n, k, d \geq 3)$ systematic linear codes that can be used for correcting every single error and detecting other error patterns. We show that there exists one code whose PUDE is upper bounded by $(n+1) \cdot [2^{n-k}-n]^{-1}$ when the transition probability is less than $2/n$. In the second part, we study the (n, k) systematic linear codes that are used for correcting some low weight-error patterns and detecting other error patterns. Suppose that $1-R > H(2\lambda)$. We show that there exists an $(n, Rn, d \geq 2\lambda n+1)$ linear code whose PUDE is closely upper bounded by $2^{-[1-R-H(\lambda)]n}$ as n approaches infinity and the transition probability is less than λ (if it is used to correct all the error patterns of weight at most λn and to detect other error patterns).

Manuscript received February 8, 1989; revised December 1, 1989. This work was presented at the IEEE 1990 International Symposium on Information Theory, San Diego, CA, January 14–19, 1990. This work was supported by the National Science Council of the Republic of China under grant NSC 78-0404-E002-05.

M.-C. Lin is with the Department of Electrical Engineering, National Taiwan University, Taipei 10764, Taiwan, ROC.

IEEE Log Number 9036388.

II. Codes for Error Detection and Single-Error Correction

Consider the ensemble Γ of all systematic $(n, k, d \geq 3)$ binary linear codes. The generator matrix of an (n, k) systematic linear code V is of the form $G = [I \quad P]$, where I is the $k \times k$ identity matrix and P is some $k(n-k)$ matrix. A necessary and sufficient condition for V to have minimum distance of at least 3 is that no two rows of P are identical and each row in P must have weight of at least 2. Therefore, the cardinality of Γ is

$$\begin{aligned}|\Gamma| &= \left[2^{n-k}-1-(n-k)\right] \cdot \left[2^{n-k}-1-(n-k)-1\right] \\ &\quad \cdots \left[2^{n-k}-1-(n-k)-(k-1)\right] \\ &= \frac{\left[2^{n-k}-1-(n-k)\right]!}{\left[2^{n-k}-1-n\right]!}. \end{aligned} \tag{1}$$

We denote the codes in Γ by $V_1, V_2, \cdots, V_{|\Gamma|}$. Let $A_{i,w}$ be the number of weight-w codewords in V_i, where $i = 1, 2, \cdots, |\Gamma|$, and $w = 0, 3, 4, \cdots, n$. Suppose V_i is used to correct every single error and detect other error patterns over a BSC with transition probability p, its PUDE is

$$P(E|V_i) = \sum_{w=2}^{n} \left[(w+1) \cdot A_{i,w+1} + A_{i,w} + (n-w+1) \cdot A_{i,w-1}\right] \cdot p^w (1-p)^{n-w}. \tag{2}$$

If the probability of choosing each code in Γ is equally likely, the average PUDE over all the codes in Γ is

$$\begin{aligned} P(E) &= \frac{1}{|\Gamma|} \sum_{i=1}^{|\Gamma|} P(E|V_i) \\ &= \frac{1}{|\Gamma|} \sum_{w=2}^{n} \left\{ \left[(w+1) \cdot \sum_{i=1}^{|\Gamma|} A_{i,w+1} \right] + \left[\sum_{i=1}^{|\Gamma|} A_{i,w} \right] \right. \\ &\quad \left. + \left[(n-w+1) \cdot \sum_{i=1}^{|\Gamma|} A_{i,w-1} \right] \right\} \cdot p^w (1-p)^{n-w}. \end{aligned} \tag{3}$$

Note that each nonzero n-tuple appears in at most $|\Gamma'|$ codes in Γ, where

$$\begin{aligned}|\Gamma'| &\leq \left[2^{n-k}-1-(n-k)\right]\left[2^{n-k}-1-(n-k)-1\right] \\ &\quad \cdots \left[2^{n-k}-1-(n-k)-(k-2)\right] \\ &= \frac{\left[2^{n-k}-1-(n-k)\right]!}{\left[2^{n-k}-n\right]!}. \end{aligned} \tag{4}$$

Thus, we have

$$\begin{aligned} &\sum_{w=2}^{n} \left[(w+1) \sum_{i=1}^{|\Gamma|} A_{i,w+1} \right] \cdot p^w (1-p)^{n-w} \\ &\quad \leq \sum_{w=2}^{n} (w+1) \binom{n}{w+1} \cdot |\Gamma'| \cdot p^w (1-p)^{n-w} \\ &\quad = |\Gamma'| \cdot n(1-p) \cdot \sum_{w=2}^{n} \binom{n-1}{w} \cdot p^w (1-p)^{n-1-w} \\ &\quad \leq |\Gamma'| \cdot n(1-p) \end{aligned} \tag{5}$$

and

$$\sum_{w=2}^{n}\left[\sum_{i=1}^{|\Gamma|}A_{i,w}\right]\cdot p^w(1-p)^{n-w} \le \sum_{w=2}^{n}\binom{n}{w}\cdot|\Gamma'|\cdot p^w(1-p)^{n-w}\le|\Gamma'| \quad (6)$$

with

$$\sum_{w=2}^{n}\left[(n-w+1)\cdot\sum_{i=1}^{|\Gamma|}A_{i,w-1}\right]\cdot p^w(1-p)^{n-w} \le \sum_{w=2}^{n}(n-w+1)\binom{n}{n-w+1}\cdot|\Gamma'|\cdot p^w(1-p)^{n-w} = |\Gamma'|\cdot np\cdot\sum_{w=2}^{n}\binom{n-1}{w-1}\cdot p^{w-1}(1-p)^{n-1-(w-1)}\le|\Gamma'|\cdot np. \quad (7)$$

Combining (4)–(7) we have

$$p(E)\le\frac{|\Gamma'|}{|\Gamma|}(n+1)\le\frac{n+1}{2^{n-k}-n}. \quad (8)$$

It follows from (8) that, for each p, there exists a code in Γ whose PUDE is at most $n+1/2^{n-k}-n$. Note that the term $p^w(1-p)^{n-w}$ is an increasing function of p if $p\le w/n$. Hence, for each code V_i in Γ, $P(E|V_i)$ is an increasing function of p if $p\le 2/n$. Therefore, we see that there exists at least one code in Γ such that its PUDE is upper bounded by

$$\frac{n+1}{2^{n-k}-n}, \qquad \text{for } p\le 2/n.$$

III. Codes for Error Detection and Multiple-Error Correction

The ensemble of all the systematic (n,k) linear codes contains $2^{k(n-k)}$ distinct codes while at most

$$\left[\sum_{i=1}^{d-1}\binom{n}{i}\right]\cdot 2^{(k-1)(n-k)}$$

of them contain nonzero codewords of weight less than d. Thus, the ensemble of all the systematic $(n,k,d\ge D)$ linear codes Γ_D contains

$$|\Gamma_D|\ge 2^{k(n-k)}-\left[\sum_{i=1}^{D-1}\binom{n}{i}\right]\cdot 2^{(k-1)(n-k)} \quad (9)$$

distinct codes. Let V_l be a code in Γ_D, and let $A_{l,w}$ be the number of codewords of weight w in V_l, where $l=1,2,\cdots,|\Gamma_D|$. Assume $D=2t+1$. If V_l is used for correcting all the error patterns of weight no more than t and detecting other error patterns, then its PUDE [4] is

$$P(E|V_l)=\sum_{w=D}^{n}A_{l,w}\sum_{i=0}^{t}\sum_{j=0}^{\min(t-i,n-w)}\cdot\left\{\binom{w}{i}\binom{n-w}{j}p^{w-i+j}\cdot(1-p)^{n-w+i-j}\right\}. \quad (10)$$

If we define $\binom{n}{i}$ as zero for $i>n$ or $i<0$, then we can replace the index term of $\min(t-i,n-w)$ in (10) by $t-i$. If each code in Γ_D is selected equally likely, by taking the average of (10) over codes in Γ_D, we have

$$P(E)=\frac{1}{|\Gamma_D|}\sum_{l=1}^{|\Gamma_D|}\sum_{w=D}^{n}A_{l,w}\sum_{i=0}^{t}\sum_{j=0}^{t-i}\cdot\left\{\binom{w}{i}\binom{n-w}{j}\cdot p^{w-i+j}(1-p)^{n-w+i-j}\right\}. \quad (11)$$

Since each nonzero n-tuple appears in at most $|\hat{\Gamma}|=2^{(k-1)(n-k)}$ codes in Γ_D, then

$$P(E)\le\frac{|\hat{\Gamma}|}{|\Gamma_D|}\sum_{w=D}^{n}\binom{n}{w}\sum_{i=0}^{t}\sum_{j=0}^{t-i}\cdot\left[\binom{w}{i}\binom{n-w}{j}p^{w-i+j}(1-p)^{n-w+i-j}\right]. \quad (12)$$

Let $i+j=m$. Then

$$\begin{aligned}&\sum_{w=D}^{n}\binom{n}{w}\sum_{i=0}^{t}\sum_{j=0}^{t-i}\left[\binom{w}{i}\binom{n-w}{j}p^{w-i+j}(1-p)^{n-w+i-j}\right]\\ &=\sum_{w=D}^{n}\sum_{m=0}^{t}\sum_{i=0}^{m}\binom{n}{w}\binom{w}{i}\binom{n-w}{m-i}\cdot p^{w+m-2i}(1-p)^{n-w-m+2i}\\ &=\sum_{w=D}^{n}\sum_{m=0}^{t}\sum_{i=0}^{m}\frac{n!}{w!(n-w)!}\cdot\frac{w!}{i!(w-i)!}\cdot\frac{(n-w)!}{(n-w-m+i)!(m-i)!}\cdot p^{w+m-2i}(1-p)^{n-w-m+2i}\\ &=\sum_{w=D}^{n}\sum_{m=0}^{t}\binom{n}{m}\sum_{i=0}^{m}\binom{n-m}{w-i}\binom{m}{i}\cdot p^{w-i}(1-p)^{(n-m)-w+i}p^{m-i}(1-p)^{i}\\ &\le\sum_{m=0}^{t}\binom{n}{m}\sum_{i=0}^{m}\sum_{w=i}^{n-m+i}\binom{n-m}{w-i}p^{w-i}(1-p)^{(n-m)-w+i}\cdot\binom{m}{i}p^{m-i}(1-p)^{i}\\ &=\sum_{m=0}^{t}\binom{n}{m}\sum_{i=0}^{m}\binom{m}{i}p^{m-i}(1-p)^{i}\\ &=\sum_{m=0}^{t}\binom{n}{m}. \end{aligned} \quad (13)$$

Thus

$$P(E)\le\frac{|\hat{\Gamma}|}{|\Gamma_D|}\sum_{m=0}^{t}\binom{n}{m}\le\frac{\sum_{m=0}^{t}\binom{n}{m}}{2^{n-k}-\sum_{i=0}^{D-1}\binom{n}{i}}. \quad (14)$$

This shows the existence of a code in Γ_D with PUDE upper bounded by (14) for $p\le(t+1)/n$. If we take D to be 3, (14) does not reduce to (8), since here we use a looser bound in estimating the size of the ensemble of codes. Note that the requirement of $2^{n-k}-n>0$ in (8) is a necessary and sufficient condition for the existence of (n,k) binary linear codes of distance of at least 3, while the requirement of

$$2^{n-k}-\sum_{i=0}^{D-1}\binom{n}{i}>0$$

in (14) is only a sufficient condition for the existence of (n,k) binary linear codes of distance at least D. From (14), we note that if

$$\sum_{i=0}^{D-1}\binom{n}{i}$$

is substantially smaller than 2^{n-k} then there exists an (n,k) code in Γ_D whose PUDE is closely upper bounded by

$$\sum_{m=0}^{t}\binom{n}{m}\cdot 2^{-(n-k)}.$$

This result agrees with our intuition, since this PUDE is the probability of error patterns which belong to $\Sigma_{m=0}^{t}\binom{n}{m}$ cosets of the standard array for a linear code as $p=1/2$.

Now we want to examine the behavior of PUDE when n approaches infinity. Let $t=\lambda n$, $k=Rn$, where $0<\lambda<1/4$. Then, $D-1=2\lambda n$. It [5] can be shown that

$$\sum_{m=0}^{\lambda n}\binom{n}{m}\le 2^{nH(\lambda)} \tag{15}$$

and

$$\sum_{i=0}^{D-1}\binom{n}{i}\le 2^{nH(2\lambda)} \tag{16}$$

where $H(\lambda)=-\lambda\log_2\lambda-(1-\lambda)\log_2(1-\lambda)$. Thus

$$P(E)\le\frac{2^{H(\lambda)n}}{2^{(1-R)n}-2^{H(2\lambda)n}}. \tag{17}$$

If $H(2\lambda)<1-R$, as n approaches infinity, (17) becomes

$$P(E)\le 2^{-[1-R-H(\lambda)]n}. \tag{18}$$

Hence, we show that for the ensemble of linear codes of length n, which are used for correcting all the error patterns of weight no more than λn and detecting other error patterns, there exists at least one code such that its PUDE is upper bounded by $2^{-[1-R-H(\lambda)]n}$ as n approaches infinity, if $1-R>H(2\lambda)$ and $p\le\lambda$. It is interesting to see that for each transmission of such a code, the probability of acceptance by the receiver is

$$P(A)\ge 1-\sum_{w=\lambda n+1}^{n}\binom{n}{w}\cdot p^w(1-p)^{n-w}. \tag{19}$$

Using the inequality (A.6) in [6], (19) yields

$$P(A)\ge 1-\left\{(p/\lambda)^{\lambda}[(1-\lambda)/(1-p)]^{1-\lambda}\right\}^n,\qquad \text{for } p<\lambda. \tag{20}$$

References

[1] S. Lin and D. J. Costello, Jr., "*Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "Concerning a bound on undetected error probability," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 235–237, 1976.

[3] S. K. Leung-Yan-Cheong, E. R. Barnes, and D. U. Friedman, "On some properties of the undetected error probabilities of linear codes," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 110–112, Jan. 1979.

[4] R. H. Deng and D. J. Costello, Jr., "Reliability and throughput analysis of a concatenated coding scheme," *IEEE Trans. Commun.*, vol. COM-35, pp. 698–705, July 1987.

[5] F. J. MacWilliams and N. J. A. Sloane, "*The Theory of Error-Correcting Codes*. New York: North-Holland.

[6] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

New Results on Self-Orthogonal Unequal Error Protection Codes

ZHI CHEN, PINGZHI FAN, AND FAN JIN

Abstract—**A lower bound on the length of binary self-orthogonal unequal error protection (UEP) codes is derived, and two design procedures for constructing optimal self-orthogonal UEP codes are proposed. Using this bound, we comment on some known codes.**

I. Introduction

In data transmission and processing, error-correcting codes can provide efficient error protection. But in many applications, not all digits are equally important, and errors in more important digits are more serious than those in less important digits. Thus, it is appropriate to use codes with unequal error protection capability.

Since such codes were first introduced by Masnick and Wolf [1], many results have been achieved [2], [3]. Usually, a decoding algorithm for such a code is complicated, so it is necessary to design UEP codes which can be implemented easily. Self-orthogonal UEP codes are therefore introduced. We first derive a lower bound for such codes, and then propose two procedures for constructing codes that are optimal among the systematic self-orthogonal UEP codes. Comparison with known codes [4] is also given.

II. Lower Bound for Self-Orthogonal UEP Codes

Definition 1: For a linear $[n,k]$ code C over the alphabet GF(q), the separation vector $S(G)=(S(G)_1,S(G)_2,\cdots,S(G)_k)$ of length k, with respect to a generator matrix G of C, is defined by

$$S(G)_i=\min\{wt(mG)|m\in GF(q)^k, m_i\neq 0\},\qquad i=1,2,\cdots,k. \tag{1}$$

The parameters of such a code are usually written as $[n,k,S(G)]$ and, in general, depend on the particular choice of the generator matrix G as well as on C.

Given a binary $[n,k]$ code, if the parity check rules are chosen such that no two codeword digits appear together in more than one parity-check equation, then the code is said to be self-orthogonal (in this correspondence, we examine self-orthogonal codes in this sense, see also Massey [5]). In addition, if the message digit m_i in such a code is checked by at least J_i parity check digits, then the component s_i of the separation vector of the code is at least J_i+1. For a self-orthogonal UEP code, the message digit m_i can be protected against $\lfloor J_i/2\rfloor$ errors with the majority logic decoding algorithm.

In many practical applications, it is more convenient to use the following definition to describe UEP codes.

Definition 2: $R=(r_1,r_2,\cdots,r_t)$ and $D=(d_1,d_2,\cdots,d_t)$ are called the code rate vector and distance vector respectively, where $d_1,\cdots,d_t$ are distinct, and $\{d_1,\cdots,d_t\}=\{S(G)_j=s_j|j=1,2,\cdots,k\}$. Let k_i be the number of message digits with the same d_i, and let $r_i=k_i/n$ be the part code rate, for $i=$

Manuscript received November 18, 1988; revised January 10, 1990. This work was supported in part by the National Natural Science Foundation of China under Grant 6873017.

The authors are with the Department of Computer Science and Engineering, Southwest Jiaotong University, Emei, Sichuan 614202, PRC.

IEEE Log Number 9035997.