Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2016 = 6.17, www.srjis.com
UGC Approved Sr. No.45269, SEPT-OCT 2017, VOL- 4/36

ON SOME PROPERTIES OF THE UNDETECTED ERROR PROBABILITY OF LINEAR CODES

Kamal Gupta

P.G. Department of Mathematics, Guru Nanak College, Ferozepur Cantt.

Abstract

A recent paper [l] discussed the 2^{-P} bound (where p = n - k) for the probability of undetected error P(e) for an (n,k) block code used for error detection on a binary' symmetric channel. This investigation is Since continued and extended and dual codes are studied. The dual and extension of a perfect code obey the 2^{-P} bound, but this is not necessarily true for arbitrary codes that obey the bound. Double-error-correcting BCH codes are shown to obey the bound. Finally the problem of constructing we obtain uniformly good codes is examined.

1. INTRODUCTION:

Leung and Hellman (1976) examined the generally accepted rule that the probability of undetected error P(ε) for an (n, k) block code, when used solely for error detection on a binary symmetric channel (BSC) with cross – over probability ε < ½, is upper bounded by 2-p, where p = n – k is the number of parity – check bits. They showed that this bound is not necessarily obeyed by linear, cyclic, or even BCH codes. However, due to the very "uniform" distribution of their codewords in binary n-space, perfect codes do obey the bound.

Cheong Barnes and Friedman [1979] In this correspondence we extended the investigation in Hellman [1976] and take a close look at extended and dual codes. several interesting results and proved, and counter examples are given to certain reasonable conjectures. It is shown that double-error-correcting BCH codes obey the 2-p bound. Codes which have small maximum P(ε) on a BSC with any ε between zero and one are discussed, and several classes of such codes are mentioned.

To be concise, we will refer to a code for which P(ε) is monotonically increasing in ε, for $0 \leq \varepsilon \leq ½$, as a proper code. Otherwise, the code will be termed improper. Note that when ε = ½, P (ε) = (2k - 1)/2n < 2-p, for any (n, k) code. Thus a proper code always obeys the 2-p bound.

2. SOME CLASSES OF PROPER CODES:

In this section we examine certain commonly used codes to determine whether or not they are proper. Unless otherwise stated, we assume $\in \leq ½$.

Proposition 1: Binary perfect codes are proper.

Proof: See Hellman [1976].

Proposition 2: Single parity – check codes are proper.

Proof: For a single parity – check code, n = k + 1. Let Ai denote the number of codewords of weight i. Then

$$P(\in) = \sum_{i=1}^{k+1} A_i \in^i (1-\in)^{k+1-i} \qquad \ldots(2.1)$$

Now

$$A_i = \begin{cases} \binom{k}{i} + \binom{k}{i-1}, & \text{if } i \text{ is even} \\ 0, & \text{otherwise} \end{cases} \qquad \ldots(2.2)$$

Substituting (2.2.2) into (2.2.1), and noting that

$$\binom{k}{i} + \binom{k}{i-1} = \binom{k+1}{i},$$

we obtain

$$P(\in) = \sum_{i=2,4,6\cdots} \binom{k+1}{i} \in^i (1-\in)^{k+1-i} \qquad \ldots(2.3)$$

Since

$$\sum_{j=0,2,4\cdots} \binom{m}{j} \in^i (1-\in)^{m-j} = [1+(1-2\in)^m]/2, \qquad \ldots(2.4)$$

we obtain

$$\mathbf{P(\in) = [1+(1-2\in)^{k+1}]/2 - (1-\in)^{k+1}} \qquad \ldots(2.5)$$

Differentiating P ($\in$) with respect to $\in$, we have

$$\mathbf{\frac{dP(\in)}{d\in} = (k+1)\,[(1-\in)^k - (1-2\in)^k]} \qquad \ldots(2.6)$$

$$\geq 0, \qquad \text{if } 0 \leq \in \leq \frac{1}{2}$$

Note from (2.6) that dP(∈)/ d∈ ≥ 0, for 0 ≤ ∈ ≤ 1, if k is odd. We shall make use of this fact later. Also, if k is even, P (∈) is maximized at ∈= 2/3.

At this point, one might wonder if adding an overall parity check bit to a proper code. A little thought indicates that this is not necessarily true: suppose we start with a proper code and start adding overall parity bits. The first overall parity bit will increase by one the weights of all odd-weight codewords (if any) and leave the weights of even-weight codewords unaltered. Additional parity bits will not affect the weights of the codewords (which now all have even weight) and only increase the blocklength. In view of Lemma 1 below, it is easy to see that an overall parity bit can convert a proper code consisting only of even-weight codewords into an improper one.

Lemma 1: If P (∈) = α∈i (1- ∈)n – i, then P (∈) is monotonically increasing for 0 ≤ ∈ ≤ i/n.

One might now ask if adding an overall parity-check bit to a proper code which contains odd-weight codewords yields an extended proper code. This is not necessarily so.

Proposition 3: The extension of a proper code containing odd-weight codewords need not be proper.

Proof: Consider the linear code consisting of the four codewords {000000, 1100000, 0011111, 1111111}. The undetected error probability for this code is given by

$$P1(\in) = \in 2\ (1 - \in)5 + \in 5\ (1 - \in)2 + \in 7, \qquad \ldots(2.7)$$

and that of the extended code is

$$P2\ (\in) = \in 2\ (1 - \in)6 + \in 6\ (1 - \in)2 + \in 8. \qquad \ldots(2.7)$$

It can be shown that P1(∈) is monotonically increasing in ∈, for 0 ≤ ∈ ≤ ½, whereas P2 (∈) is not.

Proposition 4: Extended Hamming codes are proper.

Remark: An extended Hamming code is a Hamming code with an additional overall parity check bit. It is commonly used to give the code the ability to detect double errors besides correcting single errors.

Proof: It is known Peterson [1972] that the weight enumerator for the extended Hamming code is

$$A(x) = \sum_{i=0}^{n} A_i x^i$$

$$= \frac{1}{2n}\left[(1+x)^n + (1-x)^n + 2(n-1)(1-x^2)^{n/2}\right] \quad \ldots(2.9)$$

where n = 2m, m = 2, 3, 4, …..

We can write P(∈) in terms of the weight enumerator A (x) as follows:

$$P(\in) = \sum_{i=1}^{n} A_i \in^i (1-\in)^{n-i} \quad \ldots(2.10)$$

$$= (1-\in)^n \left[A\left(\frac{\in}{1-\in}\right) - 1\right] \quad \ldots(2.11)$$

Using (2.9) in (2.11) yields

$$P(\in) = \frac{1}{2n}\left[1 + (1-2\in)^n + 2(n-1)(1-2\in)^{n/2} - 2n(1-\in)^n\right] \quad \ldots(2.12)$$

Differentiating P(∈) with respect to ∈, we obtain.

$$\frac{dP(\in)}{d\in} = (1-2\in)^{n-1} - (n-1)(1-2\in)^{n/2-1} + n(1-\in)^{n-1} \quad \ldots(2.13)$$

To prove that dP(∈)/d∈≥0, for 0 ≤ ∈ ½, it suffices to show that

$$f_l(\in) \triangleq 2l(1-\in)^{2l-1} - (1-2\in)^{2l-1} - (2l-1)(1-2\in)^{l-1} \geq 0, \quad \ldots(2.14)$$

where l ≥ 2 and 0 ≤ ∈ ≤ ½ . The reader is referred to the Appendix for a proof of (2.14).

Remark: Since it is easily shown that repetition codes and the extended Golay code are proper, we conclude that all extended binary perfect codes are proper.

Proposition 5: Maximal length codes are proper.

Proof: Let us recall that a (2m – 1, m) maximal length code (parameterized by an integer m > 2) consists of the all-zero codeword and 2m – 1 codewords of weight 2m-1. Therefore

$$P(\in) = (2^m - 1) \in^{2m-1} (1-\in)^{2^m - 2^{m-1} - 1} \quad \ldots(2.15)$$

From Lemma 1 it follows that dP(∈)/d∈ ≥ 0, for 0 ≤ ∈≤ ½.

Considering the results obtained so far, one is led to a number of speculations about the properties of proper codes. Since the single parity – check codes are the duals of the repetition codes, and the maximal length codes are the duals of the Hamming codes [1972], [1970], one might suspect the following.

Proof: It is known Bannett [1973] that the only binary perfect codes are

1. The repetition codes with odd blocklength,
2. The Hamming codes,
3. The Golay (23, 12) code.

We have already shown that the duals of (1) and (2) are proper. The dual of the Golay (23, 12) code has the generator polynomial g (x) = 1 + x2 + x5 + x8 + x9 + x10 + x11 + x12. It is easy to show that this code is proper. It is very tempting at this point to conjecture that the dual of a proper code is also proper. Unfortunately this turns out not to be the case.

Proposition 7: The dual of a proper code is not necessarily proper.

Proof: Consider the following (15, 3) cyclic code with generator matrix

$$G = \begin{bmatrix} 001 & 001 & 001 & 001 & 001 \\ 010 & 010 & 010 & 010 & 010 \\ 100 & 100 & 100 & 100 & 100 \end{bmatrix}.$$

This code consists of one codeword of weight 0, three of weight 5, three of weight 10, and one of weight 15. Its undetected error rate is $P(\in) = 3\in 5\ (1- \in)10 + 3\in 10\ (1 - \in)5 + \in 15$, which does not increase monotonically with $\in$, for $0 \leq \in \leq ½$. At $\in = ½, P(\in) = 7 \times 2\text{-}15 = 2.136 \times 10\text{-}4$, but at $\in = 1/3$ say, $P(\in) = 2.21 \times 10\text{-}4$. Thus the code defined by G is improper.

As proved in Lemma 2 below, the undetected error rate for the dual code is given by $P(\in) = 2\text{-}3\ [1 + 3\ (1 - 2\in)5 + 3\ (1 - 2\in)10 + (1 – 2\in)15 – 8\ (1 - \in)15]$, which can be shown to be monotonically increasing for $0 \leq \in \leq ½$.

Lemma 2: Let A (x) be the weight enumerator of any (n , k) linear code. Then the probability of undetected error for the dual code, used solely for error detection on a BSC with crossover probability $\in$, is given by

$$P(\in) = 2\text{-}k\ [A\ (1 - 2\in) – 2k\ (1 - \in)n]. \qquad \ldots(2.16)$$

Proof: Let B (x) be the weight enumerator of the dual code.

Then

$$P(\in) = (1-\in)^n \left[B\left(\frac{\in}{1-\in}\right) - 1 \right]. \qquad \ldots(2.17)$$

We now make use of the Mac Williams identity [1972], [1970]

$$2^k B(x) = (1+x)^n A\left(\frac{1-x}{1+x}\right). \qquad \ldots(2.18)$$

From (18),

$$B\left(\frac{\in}{1-\in}\right) = 2^{-k} (1-\in)^{-n} A(1-2\in). \qquad \ldots(2.19)$$

Substitution of (2.19) in (2.17) yields (2.16).

Motivated by the fact that the codewords of double – error – correcting BCH codes are fairly uniformly distributed in binary n-space, we have been able to establish the following result.

Theorem 1: Double – error – correcting BCH codes are proper.

Remark: This theorem is established by showing that $P(\in)$ is monotonically increasing for $0 \leq \in \leq ½$. The proof is rather long and is available from the authors upon request.

We conclude this section with the conjecture that quasi-perfect codes obey the 2-p bound.

3. UNIFORMLY GOOD CODES:

So far we have assumed that the cross-over probability of the BSC is not greater than ½. In this section, we examine some error detecting codes which perform well for any $\in$ between zero and one. One immediate observation to be made is that we cannot use a linear code which has the all-ones vector as a codeword, since than $P(\in)$ will be equal to one for $\in = 1$.

Definition: Let Ai denote the number of codewords of weight i in a certain code of blocklength n. Then the code is said to have a symmetric weight distribution if

$$A_i = A_{n-i}, \qquad 0 \leq i \leq n. \qquad \ldots(2.20)$$

The following result whose proof is straightforward will be useful in the sequel.

Lemma 3: A binary linear code contains the all-ones vector if and only if it has a symmetric weight distribution.

We now prove a result which should be useful in finding uniformly good codes.

Proposition 8: Let n be odd. Suppose we have a binary (n, k) code e with a symmetric weight distribution, and the undetected error probability of the code when used over a BSC with cross-over probability $\in$, $0 \leq \in \leq ½$, is maximum at $\in = ½$. Consider the code e' constituting only of the codewords of e with weight less than n/2. Then the probability of undetected error for code e' is upperbounded by

$$Pe(\in) < 2^{-(n-k)}, \quad \text{for } 0 \leq \in \leq 1. \qquad \ldots(2.21)$$

Remark: Code e' is not necessarily linear.

Proof: Let A' i(cj) denote the number of codewords in e' at distance i from cj. Then the probability of undetected error (for a BSC with cross-over probability $\in$) given that cj is sent is given by

$$P_e(\in | c_j) = \sum_{i=1}^{n-1} A'_i(c_j) \in^i (1-\in)^{n-i} \qquad \ldots(2.22)$$

$$\leq \sum_{i=1}^{n-1} A_i \in^i (1-\in)^{n-i} \qquad \ldots(2.23)$$

where Ai is the number of codewords of weight i in e. We have used Lemma 3 in (2.22). Inequality (2.23) follows since A' i(cj) ≤ Ai. Using (2.23) we observe that on a BSC with cross-over probability (1 - $\in$),

$$P_e(1-\in | c_j) \leq \sum_{i=1}^{n-1} A_i (1-\in)^i \in^{n-i} \qquad \ldots(2.24)$$

$$= \sum_{i=1}^{n-1} A_{n-i} (1-\in)^i \in^{n-i} \qquad \ldots(2.25)$$

$$= \sum_{i=1}^{n-1} A_l (1-\in)^{n-l} \in^l \qquad \ldots(2.26)$$

From (23) and (26) we see that Pe' ($\in$|cj) and Pe' (1-$\in$|cj) are both bounded by $\sum_{i=1}^{n-1} A_i \in^i (1-\in)^{n-i}$ and hence Pe($\in$). But Pe($\in$) < 2–(n-k), $0 \leq \in \leq ½$. Therefore

$$P_{e'}(\in) < 2^{-(n-k)}, \quad \text{for } 0 \leq \in \leq 1.$$

Comments: Assuming n is odd, the rates of the codes e and e' are k/n and (k – 1)/n, respectively. Proposition 8 shows that for certain codes, decreasing the rate by7 1/n results in a code with better P($\in$) for all $\in$, $0 \leq \in \leq 1$.

4. CONCLUSION

Those codes (referred to as proper codes) which obey a commonly used bound on undetected error probability have been examined. It has been shown that the duals and extensions of perfect codes are proper, but the duals and extensions of arbitrary proper codes need not be proper. A class of codes called uniformly good codes were defined, and a method was suggested for constructing them from well-known codes such as Hamming of BCH codes. The search for other interesting classes of uniformly good codes is an area for further research.

REFERENCES

S. K. Leung-Yan-Cheong and Martin E. Hellman, "Concerning a bound on undetected error probability," IEEE Trans. Inform. Themy, vol. IT-22. pp. 235-231, Mar. 1916.

W. W. Peterson and E. J. Weldon, Error Correction Codes. 2nd Ed. Cambridge, MA: MIT, 1972.

S. Lin. An Introduction to Error-Correcting Codes. Englewood Cliffs, NJ, Prentice-Hall, 1970.

A. Tietavainen, "On the nonexistence of perfect codes over finite fields," SIAM J. Appl. Math., vol. 24, pp. 88-96, Jan. 1973.

F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," Bell Syst. Tech. J., vol. 42, pp. 79-94, Jan. 1963.