New One-Error Detecting Codes To Binary Asymmetric Channel

R. K. Dahiya[1]*, Hardik Dahiya[2]

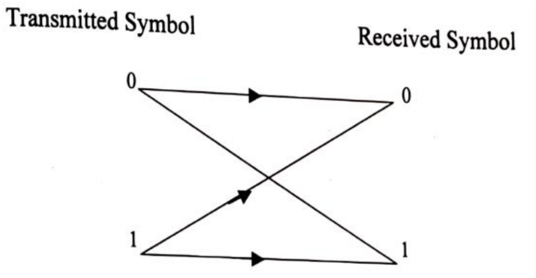
[1]*HOD, Department of Mathematics, Pt. NRS Govt. College, Rohtak -Haryana
[2]Vellore Institute of Technology, Chennai

***Corresponding Author:** R. K. Dahiya
***HOD, Department of Mathematics, Pt. NRS Govt. College, Rohtak -Haryana

Abstract:
A new codes capable of detecting one- error, when used through a binary asymmetric (or Z) channel are derived. Prefixes and suffixes are generally, used for more codes characters. Two code words distance is Hamming distance, for surety, that these codes will detect one-error. By this way, a new lower bounds is obtained for length n ≤ 20 for one-error detecting codes.

1. Introduction

Let a binary asymmetric channel (or Z-channel), which transmitted 0 is always received as correctly (0 → 0, 1 → 1), as a property. (as shown in figure I).



(Fig. I)

[The Binary Asymmetric Channel]

Hamming (1950) established the requirement of minimum distance between input code characters for error detecting and correcting codes.

Hamming distance 1 → no detection no correction
Hamming distance 2 → detects one error
Hamming distance 3 → detects and corrects one error
Hamming distance 4 → detects two errors and correct one error
Hamming distance 5 → detects and corrects two errors.

We can easily obtain the following number of code-words in binary coding system having hamming distance is ≥ 2 for different length (Table 1).

Table I Number of Code words (Hamming distance ≥ 2)

Length N	Number of Code words
2	2
3	4
4	8
5	16
6	32
7	64
8	128
9	256
10	512

In, error tolerances result, “correct all single errors and detect all double errors” is the requirement in the Symmetric channel case . But in, asymmetric channels, the resultant requirement is of the forms such as “correct all single 1-error and detect all double 1-errors”.

However, in asymmetric channels, (k + 1)-tuple 1-error may be more probable then k-tuple 0-error. For example, 110 will more likely be received as 000 then as 111. Provided

$$\alpha\beta^2 > (1-\alpha)(1-\beta)^2 \quad or \quad (1-\alpha) < \frac{\beta^2}{1-2\beta(1-\beta)}$$

In what follows, it will be assumed that the channel be highly asymmetric with $\beta >> (1-\alpha)^2$.
Rao and Chawla (1975) defined the asymmetric distance between two binary n-tuple X and Y, denoted d_a (X, Y) as

$$d_a(X, Y) = \max(r, s)$$

Where r =number of position I for which $x_i = 1$ and $y_i = 0$, s = number of position i for which $x_i = 0$ and $y_i = 1$. With the above notations, the Hamming distance d_H (X, Y) between two binary n-tuples X and y can be expressed as

$$d_H(X, Y) = r + s \quad \ldots\ldots (2.1.2)$$

This relation between the asymmetric distance d_a (X, Y) and Hamming distance d_H (X, Y) for the binary n-tuples X and Y is given by

$$d_H(X,Y) \geq d_a(X,Y) = \max(r,s) \geq \frac{(r+s)}{2} = \frac{d_H(X,Y)}{2}$$

Constantin and Rao (1979) defined, a code C detect e symmetric erros (1 → 0, or 0 → 1) if d (C) $\geq$ e + 1, and C corrects e symmetric errors if d(C) $\geq$ 2e + 1. It is thus obvious that any code, which can detect (correct) e symmetric errors, can also detect (correct) e asymmetric errors.

Theorem I (Borden 1982): Code C detects all patterns of e or fewer asymmetric errors if and only if whenever distinct codewords x and x' of C satisfy $\underline{x} > \underline{x}'$ they also satisfy $| \underline{x} \setminus \underline{x}' | \geq e + 1$.

It is interesting to compare this requirement with the combinatorial requirement arising in other coding problems. Write

$$\partial(C) = \min \{ | \underline{x} \setminus \underline{x}' | : \underline{x}, \underline{x}' \in C, \underline{x} > \underline{x}', \text{ and } \underline{x} \neq \underline{x}' \}$$

With the understanding that if all pairs of distinct codewords of C are incomplete, then ∂(C) = n + 1. Theorem I state that C detects ∂ (C) – 1 asymmetric errors.

Using the terminology introduced by Kim and Freiman (1959), we refer to the transmission ‘0 →1” as 0-errors and to the “1 → 0” transmission as 1-errors. The design of single asymmetric error (1 – error or 0 – error) detecting codes for the ideal binary asymmetric channel is the object of their paper. The method described in the sequel is the best known from the standpoint of maximizing the number of codewords in a single 1-error detecting code of a given length n.

2. Single 1-Error Detection

To construct single 1-error detecting code, we use prefixes and suffixes. We first specify code character prefixes of length m by forming all possible m-length binary sequences. For e.g. if m = 2, the prefixes would range from 00 to 11. Suffixes are generated for a given prefix by adding that prefix to code characters of (n – m) or m length. The addition is performed position by position modulo 2 and m – length code is taken to be the code word whose Hamming distance is $\geq$ 2. In this paper, author have used the terminology given by Hamming that if Hamming distance is 2, the codes will detect one error. Thus, when m = 2, 00 and 11 are code characters of Hamming distance two and 00 as prefix, will be combined with suffix 00 and 11 to give code characters 0000 and 0011.

The rule of generalization are explicitly stated below and followed by some examples. The following notation will be used

n : Code character length n > 1

m : Prefix length

$$m = \frac{n}{2}, \text{ when n is even}$$

$$m = \left(\frac{n-1}{2}\right), \text{ When n is odd}$$

Suffix is, therefore, of length n – m.
$N_2(d)$: Set of all code characters of length (n – m) whose Hamming distance is ≥ 2. N_0 is that element of $N_2(d)$ consisting of (n – m) 0's.

N_{n-m} : Number of element in $N_2(d)$.

$\oplus$: Position by position addition modulo two.
Example 1: n = 6, m = 3, $N_{n-m} = 4$
$N_2(d)$ $N_0 = 000$ $N_3 = 110$
$N_1 = 011$ $N_2 = 101$

Table – II

Prefixes of even eight	**Prefixes of odd weight**	**Suffixes**				
		$\oplus N_0$	**$\oplus N_1$**	**$\oplus N_2$**	**$\oplus N_3$**	**$\oplus N_0$**
000	001	000	011	101	110	001
011	010	011	000	110	101	010
101	100	101	110	000	011	100
110	111	110	101	011	000	111

Thus we can obtain the following codewords:

Table – III

$\oplus N_0$		**$\oplus N_1$**		**$\oplus N_2$**		**$\oplus N_3$**	
000	000	000	011	000	101	000	110
011	011	011	000	011	110	011	101
101	101	101	110	101	000	101	011
110	110	110	101	110	001	110	000
001	001						
010	010						
100	100	Total = 20 Codewords					
111	111						

Example 2:
n = 7, m = 7, $N_{n-m} = 8$
$N_2(d)$ = $N_0 = 0000$, $N_4 = 1001$
$N_1 = 0011$, $N_5 = 1010$
$N_2 = 0101$, $N_6 = 1100$
$N_3 = 0110$, $N_7 = 1111$

Table – IV

Prefixes of even eight	**Prefixes of odd weight**	**Suffixes**								
		$\oplus N_0$	**$\oplus N_1$**	**$\oplus N_2$**	**$\oplus N_3$**	**$\oplus N_4$**	**$\oplus N_5$**	**$\oplus N_6$**	**$\oplus N_7$**	**$\oplus N_0$**
000	001	0000	0011	0101	1001	1010	1010	1100	1111	0010
011	010	0110	0101	0011	1111	1000	1000	1010	1001	0100
101	100	1010	1001	1111	0011	0000	0000	0100	0101	1000
110	111	1100	1111	1010	0101	0110	0110	0000	0011	1110

Thus we can obtained the following codewords with N_0 to N_7:

$\oplus N_0$		**$\oplus N_1$**		**$\oplus N_2$**		**$\oplus N_3$**		**$\oplus N_4$**		**$\oplus N_5$**	
000	0000	000	0011	000	0101	000	0110	000	1001	000	1010
011	0110	011	0101	011	0011	011	0000	011	1111	011	1000
101	1010	101	1001	101	1111	101	1100	101	0011	101	0000
110	1100	110	1111	110	1001	110	1010	110	0101	110	0110

$\oplus N_0$		**$\oplus N_0$**		**$\oplus N_7$**		
001	0010	000	1100	000	1111	
010	0100	011	1010	011	1001	
100	1000	101	0100	101	0101	= 36 Codewords
111	1110	110	0000	110	0011	

3. Number of Codewords Obtained

The above procedure yields the following number of codewords for value of n between 2 and 20. (as in table VI)

Table VI

Number of Code Characters in Error Detecting Code	
N	Error Detecting Codewords
2	1
3	3
4	6
5	10
6	20
7	36
8	72
9	136
10	272
11	528
12	1056
13	2080
14	4160
15	8256
16	16512
17	32896
18	65792
19	131328
20	262656

4. Conclusions

The author have tried to establish a class of asymmetric 1-Error-detecting code for length 2 to 20. These codes will be better in their information rate because the Z-channel is used. More code character can be obtained for length n > 20.

5. References

1. Berger, J. M. (1961), A note on error detection codes for asymmetric channels, Inform. and Contr. 4, 68-73.
2. Constantuin, S. D. AND RAO, T. R. N. (1979), On the theory of binary asymmetric error correcting codes, Inform. and Contr. 40, 20-36.
3. Freiman, C. V. (1962), optimal error detection codes for completely asymmetric binary channels, Inform. and Contr. 5, 64-71.
4. Varshamov, R. R. (1973), A class of codes for asymmetric channels and a problem from the additive theory of numbers, IEEE Trans. Inform. Theory 19, 92-95.
5. Constantuin, S. D., And RAO, T. R. N. (1977), Concatenated group theoretic codes for binary asymmetric channels, AFIPS Conf. Proc. 46, 837-842.
6. Freiman, C. V. (1963), on the use of co-set codes in asymmetric channels, IEEE Trans. Information Theory, p. 118.
7. Gordon, T. H. (1963), Error coding bounds for the binary asymmetric channel, IEEE Trans. Information Theory, pp. 206-208.
8. Rao, T. R. N., AND Chawla, A. S. (1975), Asymmetric error codes for some LSI semiconductor memories, in "The Annual Southeastern Symposium on System Theory'," pp. 170-171.
9. Rao, T. R. N., And Constantuin, S. D. (1976), "Group Theoretic Codes for Binary Asymmetric Channels," Technical Report CS 76014, Department of Computer Science, Southern Methodist University, Dallas, Texas.
10. Varshamov, R: R., AND Tenengel'ts, G. M. (1965), Correction code for single asymmetric errors, Automat. Telemeh. 26, No. 2, 288-292.
11. Varshamov, R. R. (1966), On the theory of asymmetric codes, Cyberne. Control. Theory 10, No. 10, 901-903 [Translated from Dokl. Akad. Nauk USSR 164, No. 4 (October 1965), 757-760].
12. Varshamov, R. R. (1973), A class of codes for asymmetric channels and a problem from the additive theory of numbers, IEEE Trans. Information Theory, 92-95.
13. R. A. Silverman, "On binary channels and their cascade", *IRE Trans. on Information Theory*, vol. IT-1, pp. 19-27, December 1955.
14. R. W. Hamming, "Error-detecting and error-correcting codes", *Bell System Tech. J.*, vol. 29, pp. 147-160, April 1950.
15. M. J. E. Golay, "Binary coding", *IRE Trans. on Information Theory*, vol. IT-4, pp. 23-28, September 1954.
16. C. Y. Lee, "Some properties of non-binary error-correct codes", *IRE Trans. on Information Theory*, vol. IT-4, pp. 82, June 1958.
17. D. Slepian, "A class of binary signaling alphabets", *Bell System Tech. J.*, vol. 35, pp. 203-234, January 1956.