Malaya Journal of Matematik 4(1)(2013) 115–122

Malaya Journal of Matematik
www.malayajournal.org

MJM
an international journal of mathematical sciences with computer applications...

ISSN : 2319-3786

Error detection of irreducible cyclic codes on q-ary symmetric channel

Manish Gupta,[a,*] J.S. Bhullar[b] and O.P. Vinocha[c]

[a] *Department of Applied Sciences, GRDP College, Jida, Bathinda, India .*

[b] *Department of Applied Sciences, MIMIT, Malout, India.*

[c] *Principal, Ferozpur College of Engineering, Ferozshah, Ferozepur, India.*

Abstract

Irreducible cyclic codes are well-known classes of block codes. These codes have wide range of applications specifically in deep space. Their weight distribution of Irreducible cyclic codes is known in only a few cases specifically they are known for binary cyclic codes. Previously, it has been shown that irreducible binary cyclic codes of even dimension and their duals are either proper or not good for error detection. In this correspondence it has been established that irreducible cyclic codes in number of cases are proper when transmitted over q-ary symmetric channel. The nonzero weights of the codes treated with in this paper vary between one and four.

Keywords: binary cyclic codes, irreducible cyclic codes, weight distribution, probability of undetected error.

2010 MSC: 68P30, 94A24.

1 Introduction

Irreducible cyclic codes are the most useful block codes. These codes have numerous applications in space such as (32, 6) first-order binary Reed-Muller code was used on Mariner flight projects and the (24, 12) binary Golay code which has been proposed for a Mariner Jupiter/Saturn 1977 (MJS'77) are both (essentially) irreducible cyclic codes. These missions are part of the Mars Exploration Program of NASA. Non-binary irreducible cyclic codes could be used to conserve bandwidth for low rate, deep-space telemetry.

Irreducible cyclic codes are binary and non-binary block codes whose encoders are linear feedback shift registers, such that the polynomial that represents the feedback logic is irreducible. The weight enumerator of a block code of length n is the polynomial

$$A(x) = \sum_{i=0}^{n} A_i x^i \tag{1.1}$$

where A_i denotes the number of words of weight i in the code. The enumerator $A(Z)$ provides valuable information about the performance of the code, and is needed to compute the error probability associated with proposed decoding algorithms.

C is called an (n, k) irreducible cyclic code over F_p. It had been supposed that $q = p^s$ and $r = q^m$, where p is a prime, s and m are positive integers. A linear $[n, m, d]$ code over $GF(q)$ is a m-dimensional subspace of $GF(q)^n$ with minimum (Hamming) distance d. Let $N > 1$ be an integer dividing $r - 1$, and put

$$n = \frac{(r-1)}{N}$$

* *E-mail addresses*: manish_guptabti@yahoo.com(Manish Gupta), bhullarjaskarn@rediffmail.com (J.S. Bhullar).

Let ω be primitive element of $GF(r)$ and $\epsilon = \omega^N$. The set

$$C(r,N) = \{Tr_{\frac{r}{q}}(\alpha), Tr_{\frac{r}{q}}(\alpha\epsilon), Tr_{\frac{r}{q}}(\alpha\epsilon^{n-1}) : \alpha \in GF(R)\}$$

is called an irreducible cycle code $[n, M]$ over $GF(r)$, where $Tr_{\frac{r}{q}}$ is trace function from $GF(r)$ onto $GF(q)$ and M divides m.

Baumert and Mykkeltveit (1974) allowed to compute the weight enumerator of all $(n,k)p$-ary irreducible codes for which the integer $N = \frac{(p^k-1)}{n}$ is a prime congruent to 3 (mod 4) for which p has order $\frac{(N-1)}{2}$.

Properness of a linear error detecting code is a property which in a certain sense makes the code more appropriate for error detection over a symmetric memoryless channel than a non-proper one. This property is related to the undetected error probability of the code, which is a function of the channel symbol error probability, involving the code weight distribution. Number of authors (Leung and Hellman, 1976; Wolf et al 1982; Kasami et al 1983 and Kasami and Lin, 1984) had discussed the undetected error probability, $P_u(\epsilon)$, of linear $[n, k]$ block codes used solely for error detection on a binary symmetric channel (BSC) with bit error rate ϵ. Most of the work reported in the literature regarding the undetected error probability is restricted to binary linear codes. Although research related to the undetected error probability on the binary symmetric channel is very important but its practical value is restricted by the fact that the binary symmetric channel does not always adequately describe real communication channels (Kana and Sastry, 1978).

Error detection is used extensively in communication and computer systems to combat noise. Detection is accomplished by examining the received word. If it is a codeword, the word is accepted as error-free. If it is not a codeword, the word is rejected as being erroneous. The undetected error occurs if an error-detecting scheme fails to detect an error i.e. if the received word is a codeword different from the transmitted codeword. The probability of undetected error is given by (MacWilliams and Sloane, 1977)

$$P_u(\epsilon) = \sum_{i=1}^{n} A_i\big(\frac{\epsilon}{q-1}\big)(1-\epsilon)^{n-i} \tag{1.2}$$

where $0 \leq \epsilon \leq \frac{q-1}{q}$, A_i is the number of code words of weight i in code. For $i = 0, A_0 = 1$.

Also the weight enumerator given in (1.1) can be written as

$$A(x) - 1 = \sum_{i=0}^{n} A_i x^i.$$

Probability of undetected error $P_u(\epsilon)$ (1.2) of linear (n,k) code can be expressed as

$$\begin{aligned} P_u(\epsilon) &= \sum_{i=1}^{n} A_i\big(\frac{\epsilon}{q-1}\big)(1-\epsilon)^{n-i} \\ &= (1-\epsilon)^n \Big[A\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big) - 1\Big]. \end{aligned}$$

Code C is called good if

$$P_u(\epsilon) \leq P_u\Big(\frac{q-1}{q}\Big) = \frac{(M-1)}{q^n} \tag{1.3}$$

for all $\epsilon \in \Big[0, \frac{q-1}{q}\Big]$, where M is number of information and a code is proper if $P_u(\epsilon)$ is an increasing function for $\epsilon \in \Big[0, \frac{q-1}{q}\Big]$. Proper codes are fine for error detection. If

$$P_u(\epsilon) \leq q^{(-(n-k))}\, for\, 0 \leq \epsilon \leq \frac{q-1}{q}, \tag{1.4}$$

the code is called satisfying $q^{-(n-k)}$ bound. The code not satisfying $q^{-(n-k)}$ bound is not fine for error detection (Kasami et al 1983). Upper bound on undetected error probability for optimal linear codes is also studied by Wolf et al (1982) and Klove, (1984).

Earlier it was believed that this upper bound holds for all codes since it was assumed that $P_u(\epsilon)$ is increasing for $\epsilon \in \Big[0, \frac{q-1}{q}\Big]$ and $P_u(\epsilon)$ attains its maximum value at $\epsilon = \frac{q-1}{q}$. However, this assumption was shown to be wrong by some codes that do not obey the upper bound (Leung and Hellman, 1976) some classes of codes are known to obey this bound.

To classify codes as proper, non proper but good, or not good, often turns out to be complicated, and such a classification has been done so far for relatively few codes. Many codes which are known to be optimal or close to optimal in one sense or other, turn out to be proper, such as Maximum Distance Separable (MDS) codes, the Hamming codes, the Maximum Minimum Distance codes and their duals etc (Dodunekova et al 2008).

Our study of the codes $C(r, N)$ in this manuscript will reveal that the following irreducible cyclic codes are proper

whose length is $\frac{q^m-1}{N}$ and for any q satisfying the condition $q-1 = \frac{N}{2}(modN)$.
whose length is $\frac{q^m-1}{3}$ and for any q satisfying the condition $q = 1(mod3)$.
whose length is $\frac{q^m-1}{4}$ and for any q satisfying the condition $q = 3(mod4)$.

In this correspondence, we study the error-detecting performance of the irreducible binary cyclic codes $C(r, N)$ introduced by Delsarte and Goethals (1970) by calculating probability of undetected error $P_u(\epsilon)$. The probability has been evaluated by using weight distribution of irreducible cyclic codes derived by Ding (2009). First, we derive a new formula on the probability of undetected error for irreducible cyclic codes. Second, using this new formula, we calculated the table which shows that the $P_u(\epsilon)$ is monotonic function w.r.t error rate ϵ. The rest of this correspondence is organized as follows. In Section 2, we review some basic properties of the weight distribution of irreducible cyclic codes. In Section 3, we derive a new formula on the probability of undetected error for irreducible cyclic code. This formula plays an important role in establishing that irreducible cyclic are proper for error detection.

2 Weight distribution of irreducible cyclic codes

Determining the weight distribution of the irreducible cyclic codes in general is difficult. However, in certain special cases the weight distribution is known. Delsarte and Goethals (1970) and Baumert and McEliece (1972) have determined this polynomial in many of the simpler cases. In particular, when $k = \frac{\phi(N)}{2}$ they indicate methods that can be used to solve the problem (at least for those cases with

$$\frac{(p^k-1)}{(p-1)} = 0 \tag{2.1}$$

modulo N, as it always is for $p = 2$). Here, when N is a prime number of the form $4t + 1$ the code weight distributions are particularly nice. When N is a prime of the form $4t + 3$, things are a bit more difficult.

Baumert and Mykkeltveit (1973) determined the weight distribution for prime values of N with $N = 3(mod4)$ and $ord_q(N) = \frac{N-1}{2}$.

McEliece and Rumsey (1972) also generalized these results and showed that the weights of an irreducible cyclic code can be expressed as a linear combination of Gauss sums via the Fourier transform. Helleseht, et al (1977) investigated the weight distribution of some irreducible cyclic codes. Schmidt and White (2002) gave a characterization of irreducible cyclic codes with at most two weights. Aubry and Langevin (2005) studied the divisibility of weights in binary irreducible cyclic codes. Segal and Ward computed the weight distributions of some irreducible cyclic codes Segal and Ward (1986). Moisio and Vaananen (1999) developed two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes. Van der Vlugt (1995) investigated the weight hierarchy of irreducible cyclic codes.

However, weight distribution of only a few classes of irreducible cyclic codes is known. In contrast, little has been done on the determination of the weight distribution of the duals of irreducible cyclic codes. Ding et al (2002) determine the minimum distance and some weights of the duals of certain classes of binary irreducible cyclic codes. Ding et al (2002) show that the weight distribution of the duals of binary irreducible cyclic codes is totally determined by the cyclotomic numbers of certain order. Prior to this Niederreiter, (1977) determined the weight distribution by applying the semiprimitive cases, cyclotomy and exponential sums. Numerical examples of the weight distribution of certain minimal cyclic codes are given by MacWilliams and Seery (1981). In the semiprimitive cases and several special cases, the weight distribution of irreducible cyclic codes has been determined (Baumert and McEliece, (1972), Delsarte and Goethals, (1970), Helleseth et al (1977).

Ding (2009) described the weight distribution of the irreducible cyclic codes for all N with $2 \leq N \leq 4$ and a few other cases. The number of distinct nonzero weights in the irreducible cyclic codes dealt with in this paper varies between one and four.

3 Undetected error probability for irreducible cyclic codes

This section analyzes the properness of irreducible cyclic codes by finding undetected error probability over q-ary symmetric channel. The probability has been found from the weight distribution of irreducible cyclic codes which is given by Ding (2009).

Theorem 3.1. *Let gcd(n,N)=1, where N is even. If $q-1=\frac{N}{2}(modeN)$ and $gcd\Big(\frac{r-1}{q-1}modN, N\Big)=2$, then the set $C(r,N)$ is a $\Big[\frac{q^m-1}{N}, m, \frac{(q-1)(r-\sqrt{r})}{Nq}\Big]$ two-weight code with weight distribution*

$$A(x) = 1 + \frac{r-1}{2}x^{\frac{(q-1)(r-\sqrt{r})}{Nq}} + \frac{r-1}{2}x^{\frac{(q-1)(r-\sqrt{r})}{Nq}}. \tag{3.1}$$

Theorem 3.2. *Irreducible cyclic codes $C(r,N)$ of length $\frac{q^m-1}{N}$ are proper for any q satisfying the condition $q-1=\frac{N}{2}(modN)$.*

Proof. $P_u(\epsilon) = (1-\epsilon)^n\Big[A\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)-1\Big]$. Using the weight distribution by (3.1), we get

$$\begin{aligned} P_u(\epsilon) &= (1-\epsilon)^n\Big[1+\frac{r-1}{2}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{Nq}} + \frac{r-1}{2}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{Nq}} - 1\Big] &(3.2)\\ &= (1-\epsilon)^n\Big[\frac{r-1}{2}\Big\{\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{Nq}} + \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{Nq}}\Big\}\Big] \\ &= \frac{r-1}{2}\Big(\frac{1}{1-\epsilon}\Big)^{\frac{(q-1)(r-\sqrt{r})}{q(r-1)}}\Big(\frac{\epsilon}{q-1}\Big)^{\frac{(q-1)(r-\sqrt{r})}{Nq}}\Big[1+\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{2\sqrt{r}(q-1)}{qN}}\Big] &(3.3) \end{aligned}$$

Following tables has been derived by putting different values of r, ϵ, q and N in (3.3).

Table 1 and Table 2 shows that undetected error probability $P_u(\epsilon)$ is a monotonic function and increases with the error rate ϵ and it should obey the $q^{-(n-k)}$ bound, which proves that the codes are irreducible cyclic codes are proper for error detection. □

Theorem 3.3. *Let $q=1(mod3), p=2(mod3)$, and $m=0(mod3)$. Let $r-1=nN$, where $N=3$. If $sm=0(mod4)$, then $C(r,3)$ is an $[(r-1)/3, m, ((q-1)(r-\sqrt{r}))/3q]$ code over $GF(q)$ with weight distribution*

$$A(x) = 1 + \frac{2(r-1)}{3}x^{\frac{(q-1)(r-\sqrt{r})}{3q}} + \frac{r-1}{3}x^{\frac{(q-1)(r+2\sqrt{r})}{3q}} \tag{3.4}$$

If $sm=2(mod4)$ then $C(r,3)$ is an $[(r-1)/3, m, ((q-1)(r-2\sqrt{r}))/3q]$ code over $GF(q)$ with weight distribution

$$A(x) = 1 + \frac{(r-1)}{3}x^{\frac{(q-1)(r-2\sqrt{r})}{3q}} + \frac{2(r-1)}{3}x^{\frac{(q-1)(r+\sqrt{r})}{3q}}. \tag{3.5}$$

Theorem 3.4. *Irreducible cyclic codes $C(r,3)$ of length $\frac{q^m-1}{3}$ are proper for any q satisfying the condition $q=1(mod3)$.*

Proof. Proof of this theorem is on the same pattern as that of Theorem 3.2.
Case I: If $sm=2(mod4)$,

$$\begin{aligned} P_u(\epsilon) &= (1-\epsilon)^n\Big[1+\frac{2(r-1)}{3}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{3q}} + \frac{r-1}{3}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r+2\sqrt{r})}{3q}} - 1\Big] &(3.6)\\ &= \frac{r-1}{3}\Big(\frac{1}{1-\epsilon}\Big)^{\frac{(q-1)(r-\sqrt{r})}{q(r-1)}}\Big(\frac{\epsilon}{q-1}\Big)^{\frac{(q-1)(r-\sqrt{r})}{3q}}\Big[2+\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{\sqrt{r}(q-1)}{q}}\Big] \end{aligned}$$

Case II: If $sm=2(mod4)$,

$$\begin{aligned} P_u(\epsilon) &= (1-\epsilon)^n\Big[1+\frac{(r-1)}{3}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-2\sqrt{r})}{3q}} + \frac{2(r-1)}{3}\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r+\sqrt{r})}{3q}} - 1\Big] &(3.7)\\ &= \frac{r-1}{3}\Big(\frac{1}{1-\epsilon}\Big)^{\frac{(q-1)(r-2\sqrt{r})}{q(r-1)}}\Big(\frac{\epsilon}{q-1}\Big)^{\frac{(q-1)(r-2\sqrt{r})}{3q}}\Big[1+2\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{\sqrt{r}(q-1)}{q}}\Big] \end{aligned}$$

The values listed in Table 3 and Table 4 illustrates that undetected error probability $P_u(\epsilon)$ increases with error rate ϵ. This proves are theorem that irreducible cyclic codes $C(r,3)$ are proper. □

Theorem 3.5. *Let $q = 3(mod4)$, and let $r - 1 = nN$, where $N = 4$. If $m = 0(mod4)$, then $C(r, 4)$ is an $[(r-1)/4, m, ((q-1)(r-\sqrt{r}))/4q]$ code over $GF(q)$ with weight distribution*

$$A(x) = 1 + \frac{3(r-1)}{4} x^{\frac{(q-1)(r-\sqrt{r})}{4q}} + \frac{r-1}{4} x^{\frac{(q-1)(r+3\sqrt{r})}{4q}} \tag{3.8}$$

If $m = 2(mod4)$ then $C(r, 4)$ is an $[(r-1)/4, m, ((q-1)(r-3\sqrt{r}))/4q]$ code over $GF(q)$ with weight distribution

$$A(x) = 1 + \frac{(r-1)}{4} x^{\frac{(q-1)(r-3\sqrt{r})}{4q}} + \frac{3(r-1)}{4} x^{\frac{(q-1)(r+\sqrt{r})}{4q}}. \tag{3.9}$$

Theorem 3.6. *Irreducible cyclic codes $C(r, 4)$ of length $\frac{q^m-1}{4}$ are proper for any q satisfying the condition $q = 3(mod4)$.*

Proof. Case I: If $m = 0(mod4)$,

$$\begin{aligned} P_u(\epsilon) &= (1-\epsilon)^n \Big[1 + \frac{3(r-1)}{4} \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-\sqrt{r})}{4q}} + \frac{r-1}{4} \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r+3\sqrt{r})}{4q}} - 1\Big] \qquad (3.10) \\ &= \frac{r-1}{4} \big(\frac{1}{1-\epsilon}\big)^{\frac{(q-1)(r-\sqrt{r})}{q(r-1)}} \big(\frac{\epsilon}{q-1}\big)^{\frac{(q-1)(r-\sqrt{r})}{4q}} \Big[3 + \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{\sqrt{r}(q-1)}{q}}\Big] \end{aligned}$$

Case II: If $m = 2(mod4)$,

$$\begin{aligned} P_u(\epsilon) &= (1-\epsilon)^n \Big[1 + \frac{(r-1)}{4} \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r-3\sqrt{r})}{4q}} + \frac{3(r-1)}{4} \Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{(q-1)(r+\sqrt{r})}{4q}} - 1\Big] \qquad (3.7) \\ &= \frac{r-1}{4} \big(\frac{1}{1-\epsilon}\big)^{\frac{(q-1)(r-3\sqrt{r})}{q(r-1)}} \big(\frac{\epsilon}{q-1}\big)^{\frac{(q-1)(r-3\sqrt{r})}{4q}} \Big[1 + 3\Big(\frac{\epsilon}{(1-\epsilon)(q-1)}\Big)^{\frac{\sqrt{r}(q-1)}{q}}\Big] \end{aligned}$$

The values listed in Table 5 and Table 6 illustrates that undetected error probability $P_u(\epsilon)$ increases with error rate ϵ. This proves are theorem that irreducible cyclic codes $C(r, 3)$ are proper. □

4 Conclusion

Irreducible cyclic codes are of practical interest as they have been used in transmission of data. In this work we had examined the performance of these codes in terms of probability of undetected error when codes are transmitted through q-ary symmetric channel. It has been substantiated that $C(r, N)$ for $2 \le N \le 4$ irreducible cyclic codes are proper codes.

References

1. Aubry, Y., & Langevin, P, On the weights of binary irreducible cyclic codes, *Proc. workshop on Coding and Cryptography*, Bergen, Norway, (2005), pp. 161-169.

2. Baumert, L. D. & McEliece, R. J, Weights of irreducible cyclic codes, *Inform. Contr.*, 20(1972), pp. 158-175.

3. Baumert, L. D., & Mykkeltveit, J, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.*, 16(1973), pp. 128-131.

4. Baumert, L. D., & Mykkeltveit, J, Weight Distribution Of Some Irreducible Cyclic Codes, *JPL Technical Report*, XVI(1974), pp. 32-1526.

5. Delsarte, P., & Goethals, J. M, Irreducible binary cyclic codes of even dimension, *Proc. 2nd Chapel Hill Conf. Combinatorial Mathematics and Its Applications*, Chapel Hill, NC, (1970), pp. 100-113.

6. Ding, C, The weight distribution of some irreducible cyclic codes, *IEEE Trans. Inf. Theory*, 55(3)(2009), pp. 955-960.

7. Ding, C., Helleseth, T., Niederreiter, H. & Xing, C, The Minimum Distance of the Duals of Binary Irreducible Cyclic Codes, *IEEE Trans. Inf. Theory*, 48(3)(2992), pp. 2679-2689.

8. Dodunekova, R., Dodunekov, S., & Nikolova, E, A survey on proper codes, *Disc. Appl. Math.*, 156(9)(2008), pp. 1499-1509.

9. Helleseth, T., Klove, T. & Mykkeltveit, J, The weight distribution of irreducible cyclic codes with block lengths $n_1(((q^l - 1/N))$, *Discr. Math.*, 18(1977), pp. 179-211.

10. Kana, L. N., & Sastry, A. R. K, Models for channels with memory and their application to error control, *Proc. IEEE*, 66(1978), pp. 724-744.

11. Kasami, T., & Lin, S, On the probability of undetected error for the maximum distance separable codes, *IEEE Trans. Commun.*, COM-32(1987), pp. 998-1006.

12. Kasami, T., Klove, T. & Lin, S, Linear block codes for error detection, *IEEE Trans. Inform. Theory*, IT-29(1)(1983), pp. 131-136.

13. Klove, T, The Probability of Undetected Error When A Code Is Used For Error Correction and Detection, *IEEE Trans. Inform. Theory*, IT-30(2)(1984), pp. 388-392.

14. Leung C.,& Hellman M. E, Concerning a bound on undetected error probability, *IEEE Tmns. Inform. Theory*, IT-22(2)(1976), pp. 235-237.

15. MacWilliams, F. J. & Seery, J, The weight distributions of some minimal cyclic codes, *IEEE Trans. Inform. Theory*, IT-27(1981), pp. 796-806.

16. MacWilliams, F. J., & Sloane, N. J. A, *The Theory of Error-Correcting Codes*, New York North Holland, 1978.

17. McEliece, R. J., & Rumsey, H. Jr, Euler products, cyclotomy, and coding, *J. Number Theory*, 4(1972), 302-311.

18. Moisio, M. J., & Vnen, K. O, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, *IEEE Trans. Inf. Theory*, 45(3)(1979), pp. 1244-1249.

19. Niederreiter, H, Weights of cyclic codes, *Inform. Contr.*, 34(2)(1977), pp. 130-140.

20. Schmidt, B., & White, C, All two-weight irreducible cyclic codes, *Finite Fields Appl.*, 8(1)(2002), pp. 1-17.

21. Segal, R., & Ward, R. L, Weight distributions of some irreducible cyclic codes, *Math. Comput.*, 46(173)(1986), pp. 341-254.

22. Vlugt, M. V. D, On the weight hierarchy of irreducible cyclic codes, *J. Comb. Theory Ser. A*, 71(1)(1995), pp. 159-167.

23. Wolf, J. K., Michelson, A. M., & Levesque, A. H, On the probability of undetected error for linear block codes, *IEEE Trans. Commun.*, COM-30(1982), pp. 317-324.

Table 1: Undetected Error Probability $P_u(\epsilon)$ of $[39, 2, 36]$ cyclic irreducible code

r	ϵ	q	N	$P_u(\epsilon)$
625	0.1	25	16	7.05972E-84
625	0.2	25	16	5.40861E-73
625	0.3	25	16	1.3363E-66
625	0.4	25	16	4.84733E-62
625	0.5	25	16	1.76756E-58
625	0.6	25	16	1.53968E-55
625	0.7	25	16	5.16578E-53
625	0.8	25	16	9.22568E-51
625	0.9	25	16	1.27255E-48

Table 2: Undetected Error Probability $P_u(\epsilon)$of $[21, 2, 18]$ cyclic irreducible code

r	ϵ	q	N	$P_u(\epsilon)$
169	0.1	13	8	3.45333E-36
169	0.2	13	8	1.00144E-30
169	0.3	13	8	1.65956E-27
169	0.4	13	8	3.35991E-25
169	0.5	13	8	2.18149E-23
169	0.6	13	8	7.04171E-22
169	0.7	13	8	1.45259E-20
169	0.8	13	8	2.34179E-19

Table 3: Undetected Error Probability $P_u(\epsilon)$of $[21, 3, 14]$ cyclic irreducible code

r	ϵ	q	$P_u(\epsilon)$
64	0.2	4	1.67E-15
64	0.3	4	5.33E-13
64	0.4	4	3.31E-11
64	0.5	4	8.51E-10
64	0.6	4	1.28E-08
64	0.7	4	1.48E-07
64	0.8	4	4.3E-06
64	0.9	4	0.003408

Table 4: Undetected Error Probability $P_u(\epsilon)$of $[21, 3, 12]$ cyclic irreducible code

r	ϵ	q	$P_u(\epsilon)$
64	0.2	4	1.83866E-13
64	0.3	4	5.32745E-13
64	0.4	4	3.31373E-11
64	0.5	4	8.51366E-10
64	0.6	4	1.27745E-08
64	0.7	4	1.47605E-07

Table 5: Undetected Error Probability $P_u(\epsilon)$of $[20, 4, 12]$ cyclic irreducible code

r	ϵ	q	$P_u(\epsilon)$
81	0.1	3	8.66909E-20
81	0.2	3	6.85958E-11
81	0.3	3	4.33931E-12
81	0.4	3	4.7521E-10
81	0.5	3	1.89687E-08
81	0.6	3	4.33238E-07

Table 6: Undetected Error Probability $P_u(\epsilon)$of $[12, 4, 6]$ cyclic irreducible code

r	ϵ	q	$P_u(\epsilon)$
49	0.1	7	1.59094E-20
49	0.2	7	7.11832E-17
49	0.3	7	1.02086E-14
49	0.4	7	3.61778E-13
49	0.5	7	6.03604E-12
49	0.6	7	6.36294E-11
49	0.7	7	5.0283E-10
49	0.8	7	3.52614E-09

Received: January 18, 2013; *Accepted*: June 06, 2013

UNIVERSITY PRESS