EFFICIENT CODES WITH CLASS ERRORS OF SK-METRIC & POLYNOMIAL POWER-PRODUCT COMPOSITION FOR CODES

Synopsis of the Thesissubmittedinfulfilmentoftherequirementsfortheˆ Degreeof

DOCTOR OF PHILOSOPHY

By

Ankita Gaur
(Enrolment No. 10408042)

DepartmentofMathematics

JAYPEEINSTITUEOFINFORMATIONTECHNOLOGY(Declar
edDeemedtobeUniversityU/S3ofUGCAct)
A-10,SECTOR-62,NOIDA,INDIA

May 2014

1. INTRODUCTION

In 1948, Claude E. Shannon published a paper entitled "The Mathematical Theory of Communication" in *Bell System Technical Journal* [27]. His paper gave birth to the twin disciplines of information theory and coding theory. This paper by Shannon is a seminal paper in the new-branch of 'Information Theory'. In fact Shannon is considered to be the father of Information theory. The paper considers problems of communication and, as the title says, gives mathematical foundations of the subject. In this fundamental work he used tools of probability theory.

In a communication system, information is sent from one point to another, very often in a noisy environment. In Shannon's paper, the model of a communication system represented in following figure is considered.

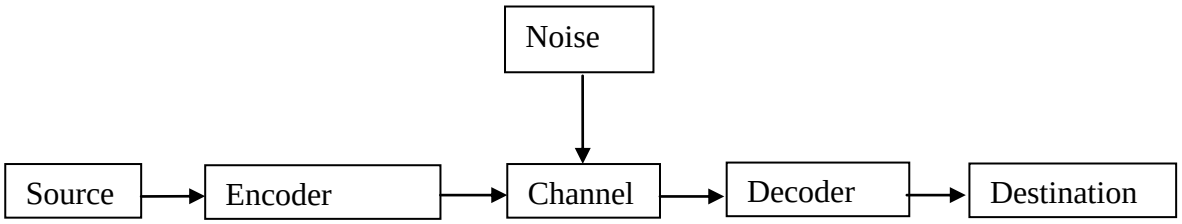

FIGURE - COMMUNICATION SYSTEM

In this model, a message is generated at the source, encoded in the channel symbols and is transmitted over the channel. During the transmission, the channel having noise, the message sent may be corrupted, so that the received message may be different from the one transmitted. The receiver then, following the decoding scheme, tries to recover the message sent.

Shannon characterised:

1. Source in terms of messages with their probabilities of occurrences;
2. Channel in terms of conditional probabilities of symbols received and sent;
3. Information in terms of a measure called 'entropy.'

Shannon introduced fundamental concepts about 'information' from the communication point of view and digital transmission. With the key ideas of entropy and

capacity of the channel, Shannon proved several results. The fundamental theorem, which is at the philosophical foundation of coding theory states:

Given an information source and a communication channel, there exists acoding technique such that:

- by properly encoding, the information can be transmitted over a noisy channel at any rate less than the channel capacity
- the transmission will have an arbitrarily small probability of error tending to zero.

Shannon's this famous theorem guaranties the existence of codes for reliable communication over unreliable channels. The transmission will have an arbitrarily small number of errors - even if the channel is noisy [1].

The theory of error correcting codes was developed to achieve what is promised by Shannon's fundamental theorem. In initial stages, work progressed for developing efficient variable length codes over noiseless channels and 'unique decodability' came up as the main concern that was ideally resolved by Kraft inequality and Huffman codes.

The work in the area of error correcting codes began with highly significant paper of Hamming [13]. By considering all messages of constant length the problem of unique decidability was by-passed and by adding redundant digits state was mathematically set to correct/detect additive errors. With readily available linear algebraic tools identified by Slepian [33], there emerged the discipline 'Algebraic Coding Theory.' A significant short paper by Golay [12] in 1949 added to deeper search in construction of multiple error correction. .

Shannon's colleague Richard Hamming was an American mathematician whose work had much implication for computer science and telecommunications. He introduced the basic concepts of linear parity checks, parity check matrix, and generator matrix for constant length codes. His contribution includes the Hamming codes, Hamming sphere or Hamming bound and Hamming distance [13].

Hamming had been labouring on error correction for early computers even before Shannon's 1948 paper, and he made some of the first breakthrough on coding theory. R.W. Humming's "Error Detecting and correcting codes" first published paper on error detection and error correction. Richard Hamming won the Turing Award in 1968 for his work at Bell

Labs in numerical methods, automatic coding systems, and error-detecting and error-correcting codes. He invented the concepts known as Hamming codes, Hamming windows, Hamming numbers, and Hamming distance [13].

The objective of channel coding is to construct encoders and decoders in such a way as to effect:

1. fast encoding of massage;
2. easy transmission of encoded message;
3. fast decoding of received message;
4. maximum transfer of information per unit time;
5. maximal detection or correction capability.

Coding theory is the branch of mathematics concerned with transmitting data across noisy channels and recovering the message sent.

Basically, the term coding is associated with:

- Error-Control Coding: This area concerned with two most important parts Error detection coding and error correction coding.
- Error correction coding: The meaning of error correction coding is to correct the data transmitted through a communication channel based upon received data or we can say that this error correction coding concerned with improving reliability of communication over noisy channels. This is achieved by adding redundancy.
- Cryptography (or Cryptology) that is concerned with security, privacy or confidentiality of communication over an insecure channel[38].

Investigations taken in this thesis will broadly fall in the category of error-correcting codes.

Major initial achievements:

- The notation of error correction was introduced by R.W. Hamming (1950) [14].
- Linear codes were independently discussed by D. Slepian [33].

- Cyclic codes are discovery of E. Prang [24] in 1957, I.S. Reed and G. Solemon [25]; BCH codes are due to R K Bose, D.K Ray Choudhari [4]; and A. Hocquenghem [15].
- Reed Muller constructed an important class of codes and invented the notation of threshold decoding [21].

2. LITERATURE REVIEW

This part of the synopsis contains two sections. In first section we go over the literature on metrics, bounds on distance and bounds on parity check digits and perfect codes and in second section we review composition of codes over existing codes.

(i) METRICS OR DISTANCES, BOUNDS AND PERFECT CODES

In error control coding theory metric (or distance) is a key instrument. There are several types of distances discovered by researchers that are used in construction of codes [9, 11]. It started with important and most commonly used metric due to Hamming [13] basically for binary channel. It has been straight forwardly used for non-binary cases, resulting in avoidable.

Another important metric was introduced by Lee [19]. The Lee metric is defined over the ring of integer's residue modulo *q*. In case of phase modulation scheme when phase modulated signals are transmitted through additive Gaussian noisy channel, the Lee metric is quite relevant. In the coding theoretic literature Lee metric is to be considered as a way to analyze codes over large alphabets applied to phase modulation [2, 21].

Over *GF (2)* or *GF* (3), where *GF* stands for Galois field Hamming metric and Lee metric make no difference. Both these distances over $GF(q)$ are of ad-hoc nature. A systematic approach was undertaken by Sharma and Kaushik [18], giving all possible distances between vectors over $GF(q)$. Sharma-Kaushik found a whole class of distance, that comprises Hamming and Lee distances as particular cases. By taking partitions of Z_q into nonempty disjoint subsets $B_0, B_1, ..., B_{m-1}$, where *m* is an integer greater than or equal to 2,satisfying some certain conditions. In this metric weight of an element keep up a

correspondence to the partitions of Z_q, because each element acquires the weight of the class to which the element belongs in partitions [29].

Bounds play an important role in coding theory. In terms of bounds on minimum distance notable contributions have been given by Hamming [13], Varshamov [37], Gilbert [11], Plotkin [23] and Elias [9](Refer Peterson & Weldon 1972) [21].By using linear programming techniques McEliece [20] drive the best upper bound on minimum distance for large length codes.

(ii) COMPOSITION OF CODES

Linear algebra and in particular vector spaces are important mathematical structures and have numerous applications. There are areas, for example coding theory, finite geometries and statistical theory of designs, where vector spaces provide basic foundations. There it is felt that higher order and more efficient structures can be developed with advantage by suitably composing the lower order structures. There is thus interest in developing new mathematical composition laws on vectors, matrices and polynomials. Elias [9] used Kronecker product of matrices to develop higher efficiency codes by combination of lower order codes. The method was powerful, but it could develop only a sparse class of product codes and the all important duality property was lost. Sharma [31], introduced a new concept of matrix-multiplication called the 'partitioned product of matrices', and obtained a rather large class of 'rank-partitioned product codes' in which the duality property was preserved. Cyclic codes, as is known, are ideally suited for implementation through shift registers. Most important codes like BCH, Goppa codes etc. are cyclic codes, which are best characterized through their generator polynomials [21]. Composing higher order cyclic codes from lower order codes in terms of their generator polynomials has not been explored at any length. The reason for not been able to do that is that there does not exist a method of multiplying two polynomials leading to what may be used to consider 'product of two cyclic codes' [39,5].

3. OBJECTIVE OF THE STUDY

- Identification actually occurring errors - partial in terms of SK-Metric – matching the channel.

- Efficiency studies for different kinds of error patterns in the form of bounds over the parity checks.
- Developing codes for designed error patterns and in particular study of the perfect codes.
- Reliability consideration in the form of probability of error for codes designed for specific errors under channel characteristics.
- Developing codes correcting higher level errors by composing those of lower orders. Using existing and developing new algebraic tools for doing so;
- Introducing a new product of two polynomials, called 'Ordered Power Product' of two polynomials that helps in developing new composition codes.
- Studying algebraic properties; applications of Ordered Power Product of polynomials in Coding Theory.
- Developing New Class of Cyclic & quasi-cyclic codes using Ordered Power Product of Polynomials.

4. THESIS OUTLINE

CHAPTER 1

INTRODUCTION & LITERATURE SURVEY

First chapter of the thesis contains a brief history of coding theory some definitions; some relevant results on bounds; perfect codes; construction of codes by composition of already existing codes. A brief overview of linear block codes and cyclic codes is also included in this chapter. The chapter also briefly gives an account of the work carried out later chapters.

CHAPTER -2

CODES CORRECTING LIMITED PATTERNS OF RANDOM ERRORS USING SK-METRIC

With the advancement of information technology coding theory is having new challenges. This is because the communication channels, the automata or the electronic devices, where they find use have varying characteristics. The errors patterns differ. Theory of

error control coding started simply with binary code words of fixed length, with basically three parameters, namely the number information digits, check digit and Hamming distance between *n*-tuples. Errors considered were random errors and the burst errors. When studies were extended to *q*-nary case these things continued without further necessary refinement. A single error continued to be an error in any position of any magnitude. The cause of this can be traced in the inbuilt nature of Hamming distance. Lee distance [19], yet another distance is also fixed in nature, with limited scope for study. Mainly in two directions work progressed, these related to optimality considerations and construction of codes capable of correcting a certain number random error correcting codes. Practically all designed distance codes, BCH, Goppa, Helgert, turned out to be 'bad', with rate falling with increasing length that is asymptotically.

Error control coding now being not limited to distant communication alone, broadening of the mathematics was needed which can suitably match the characteristics of the device for which the coding was required and can consider correction of only those patterns that need to be corrected rather than have the wasted capacity of correcting non-errors by default.

Sharma and Kaushik (SK) investigated the question of other possible different ways of defining distances/metrics over $Z_q = \{0,1,2,...,q-1\} \bmod q$, when $q > 2$. They found a whole class of possible distances defined over Z_q, by considering a special class of partitions of Z_q, satisfying certain conditions [24].

This class of SK distances, besides being rich in choice for properly matching the channel, provides possibilities of handling a wide variety of errors, which was not possible with Hamming distance or even Lee distance considerations. Hamming and Lee metrics are in fact the particular rather extremal cases of SK-studies [18, 26].

With nature of errors vastly different and SK metric, it is possible to consider codes which will have well defined error characteristics and will be far more efficient then is otherwise possible with Hamming distance consideration [32]. Since only those errors patterns of a given weight that form part of the total error patterns of that weight are considered for correction, we call them 'codes correcting partial errors.' This is undertaken in this chapter.

In this chapter we introduced the idea of partial error correction and obtained lower bounds for a variety of partial-error-correction and gave some examples of partial error correcting codes.

The Chapter is based on my following published paper:

- **Gaur A.** and Sharma B.D., "*Codes Correcting Limited Patterns of Random Error using SK-metric*" Cybernetics and Information Technologies, vol.13, No. 1, pp. 34-45, 2013.

CHAPTER-3

UPPER BOUND ON CORRECTING PARTIAL RANDOM ERRORS

In this chapter continuing random-error-correction with SK-metric considerations, a class of errors are studied, which in some sense are 'part' of the class of errors those that may have arisen from Hamming considerations. The chapter contains a sufficient condition for correcting error of a certain number of partial random errors and some examples based on the results. Results derived under Hamming considerations follow as particular cases from this study, and those for Lee metric can also be directly obtained.

The Chapter is based on my following published paper:

- **Gaur A.** and Sharma B.D., "*Upper Bound on Correcting Partial Random Errors*" Cybernetics and Information Technologies, vol.13, No. 3, pp. 41-49, 2013.

CHAPTER-4

A BROAD CLASS OF ADDITIVE ERROR CODING, CHANNELS AND LOWER BOUND ON THE PROBABILITY OF ERROR FOR BLOCK CODES USING SK-METRIC

In coding theory developing codes keeping the word lengthminimum is the main issue. While number of information digits account for the number of messages and cannot be minimized in block coding, redundant digits that are required to imbue correction/detection capabilities, for efficient transmission, are to be kept minimum and in no case not more than

enough for designed errors. There is quite an extensive study on lower and upper bounds on the number of parity-checks for codes correcting differently designed errors, mainly for random and burst errors for several variations. Mostly these bounds are combinatorial or algebraic in nature and in obtaining these bounds, probabilistic nature of digital errors is not taken into considerations. However, reliability of performance of a code demands that probability of errors and bounds on it be studied. Feinstein, Shannon (1958), Fano (1961), and Gallager (1965) have shown that for discrete memoryless channels, block coding and decoding schemes exist for which the error probability approaches zero exponentially with increasing block length for any given data rate less than channel capacity [21]. Shannon and Gallager [27] presented lower bounds for minimum error probability that can be achieved through the use of block coding on noisy discrete memoryless channels. For this purpose channel matrices along with error patterns are considered. In 2002, new lower bounds were derived on the error probability in coded communication when using maximal likelihood decoder [7]. In 2006 tightened upper bounds were derived on the error probability of binary linear block codes, under maximum-likelihood decoding, where the transmission takes place over an arbitrary binary-input output-symmetric (MBIOS) channel [36].

In this chapter using SK-metric approach we generalized the idea of additive errors by introducing a broad class of 'Class-additive errors.' In the setting of SK-distances and error probabilities, we generalized the concept of 'binary-symmetric-channel' what is '*q-nary-SK-Metric Symmetric Channel*,' studied the probabilistic aspects of error controlling codes and reported some results on bounds on probability of error and gave some examples for block codes developed on the SK- Metric Channel.

The Chapter is based on my following published paper:

- **GaurA.** and Sharma B.D., "*A Broad Class of Additive Error Coding, Channels and Lower Bound on the Probability of Error for Block Codes using SK- Metric*," International Journal of Applied Mathematics andStatistics, volume 52, Issue 1,pp 119-131,2014.

CHAPTER-5

PERFECT CODES USING CLASS METRIC

Coding theorists are greatly enamoured with perfect codes. There has been extensive research on existence and non-existence of perfect codes under Hamming distance, ending in a small class of perfect codes [15]. It may be mentioned that a code is completely devised if we are able to construct a parity check matrix H for it. Use of SK-metric and introducing the requirement of class-errors, the classes of perfect codes for these errors present a challenge. We know that a code capable of correcting error of class weight one should have minimum class weight at least three. In this chapter we obtained bounds on the number of parity check digits for codes correcting errors of SK-weight

- one on *t* positions
- two or less on t positions

over Z_q, $(q \geq 7)$ *a prime* respectively. We also examined these bounds with equality to check for perfect codes and have shown the existence of perfect codes correcting error in *t* positions of SK- weight-1 over Z_7, and perfect codes correcting errors of SK-weight -2 or less over Z_{13} .

The Chapter is based on my following published paper:

- **Gaur A.**and Sharma B.D. "*Perfect Codes Using Class Metric*", International Journal of Research in Information Technology, Volume 1, Issue 8, pp. 81-90, August, 2013.

CHAPTER-6

CODES OBTAINED BY COMBINATION OF EXISTING CODES

i. A NEW CLASS OF CYCLIC CODES USING ORDERED POWER PRODUCT OF POLYNOMIALS (OPP)

In this chapter, we start by introducing a new product of two polynomials defined over a field. It is a generalization of the ordinary product. For convenience we call the two

polynomials as outer and inner polynomials. The new defined product then results in non-overlapping segments obtained by multiplying it with coefficients of outer polynomials and expanding powers of the variable. It is called *'Ordered Power Product'* and has elegant algebraic properties leading to new algebraic structures.

The first section of this chapter includes some applications of the above concepts in developing product of two cyclic codes, in terms of the new product defined by us of two polynomials; the 'Ordered Power Product' of two polynomials in introduced and its algebraic properties; applications of Ordered Power Product of polynomials in coding theory and an example is given to illustrate the a cyclic code arising from the OPP of two cyclic codes.

ii. ORDERED POWER PRODUCT OF POLYNOMIALS AND PRODUCT QUASI CYCLIC CODES

Quasi-cyclic (QC) codes are an important class of linear codes and have some good algebraic structure. Quasi-Cyclic codes were introduced by Townsend and Weldon [35]. This was followed shortly thereafter by the works of Karlin [16, 17] and Chen [6]. Since then extensive research has been done by Bhargava [3, 34].

The construction of good codes has almost as long a history as coding theory itself. Coding is now required not only for communication but in all electronic items, automatic devices remote control systems, etc. In various applications, we need longer or larger codes, which are easily implementable. Search for longer length code is a difficult exercise and such codes independently developed tend to be inefficient. It has therefore been tried to generate such codes by composition of smaller codes. There are various ways in which codes can be combined to give new codes. From the beginning of coding theory many rules to build code with larger size or longer length from codes of smaller size or shorter length have been proposed, some of them have become standard construction in coding theory. A method of combination, called Kronekr product codes, was suggested by Peter Elias in 1954 [9]. A rather powerful generalization of product-codes has later been studied by Sharma [31]. We obtained some result for quasi cyclic codes using the newly defined OPP in this section of the chapter.

The Chapter is based on my following published paper:

- **Gaur A.** and Sharma B.D., "*A New Class of Cyclic Codes Using Ordered Power Product of Polynomials",*Journal of Applied Mathematics & Informatics, Vol.32, N0.3-4 (May, 2014)

CHAPTER-7

CONCLUSION & FUTURE SCOPE

Coding applications have grown rapidly in the past several years. This area of applied mathematics includes the study and discovery of various coding schemes that are used to correct the errors that are introduced during data transmission. There are various types of errors and a number of techniques for correction of these errors under Hamming metric for both binary and non binary cases. Hamming distance in non-binary cases is just not capable of considering errors, which are limited in other ways. Thus from both mathematical as well as from practical considerations other than Hamming metric is to be employed. All such distances over $GF(q), q > 3,$ are available through SK-partitions. To correct only those patterns that need to be corrected rather than have the wasted capacity of correcting non-errors by default, we have considered new types of error pattern using under SK-metric, and have studied a largely extended wider class of codes.

The lower bounds on redundancy or upper bounds on word length for specified limited patterns of errors, lays down the ideal situation for existence of such codes. The choices provided by use of SK-partitions and SK-distances provide a choice of metrics, including that for Hamming distance, matching the channel characteristics. It seems quite possible to extend this to constructions of codes correcting limited patterns of errors.

Mathematicians and Coding theorists have remained quite enamored with search of prefect codes. Under Hamming distance, there are only two rather trivial such classes. Search of perfect codes under new error patterns has been undertaken. Obtained bounds on the number of parity check digits for correcting errors on *t* positions of SK-weight -1, SK-weight two or less over $Z_q, (q \geq 7)$ *a prime* respectively. We have investigated the existence of perfect codes correcting error in *t* positions of SK- weight-1 over $Z_7,$ and perfect codes

correcting errors of SK-weight -2 or less over Z_{13}. While search has been quite rewarding, the search for specific values of q is bound to enrich the class of what may be termed 'special perfect codes.'

Channel is a physical medium through which information is transmitted. Probabilistic being the nature of noise, with all the care in designing codes correcting designed errors, there is a chance of errors. Thus proper characterization of channel for correction criteria, in our case SK-metric, is required for reliability, that is probability of error. We have defined a *q*-nary symmetric channel which is compatible with the SK - partition. This channel is a generlization of widely used concept of Binary-Symmetric Channels. We have denoted this *q*-nary symmetric channel for SK-partition $\wp$ by 'q$\wp$SC'.

We have results on probabilities of errors for a code designed for different classes of errors.

With generalization of additive errors and of symmetric channel for the new setting under SK-studies, there are several other possibilities that arise for further studies.

Another area of challenge for coding theorists is that of developing codes with larger number of errors. BCH and some other designed codes turn out to be inefficient for increasing number of error. Small codes with desired error correction capabilities can be easily developed; developing large codes presents a real practical problem. A practical way to obtain large codes is to obtain them by suitable composition of those of shorter lengths. Our strategy is to build codes with larger size or longer length from code of smaller size or shorter length. We introduced a new kind of product of polynomials defined over a field. We have called it 'Ordered Power Product' (OPP). OPP has wider implication in abstract algebra, that we have indicated. Using the new type of product of polynomials, for the first time in the literature, we have defined a new product of two cyclic codes and devise a method of getting a cyclic code from the 'ordered power product' of two cyclic codes. This amounts to developing new product type of codes, which are more efficient.

Our studies and ideas provide lead to several areas for continued research. In brief we envisage these as follows:

- Consider other bounds in particular Low rate bound and Linear programming bound, for codes correcting limited patterns of random errors using SK- metric and construction of codes.

- In continuation to ideas in Chapter 4, explore Coding theorems and error bounds for ‘q $\wp$ SC’ channel.
- Generalization of Reed-Solomon, BCH and other important codes for *q*-nary channels in terms of distances arising from SK-Partitions.
- Search for more perfect and quasi perfect codes under generalized distances.
- Exploring the possibility of partitioned product cyclic codes and their further studies.
- Study of Unequal error protection code under SK-Metric.

REFERENCES

[1] Ash R.B., "*Information Theory*," Wiley, New York, 1965.

[2] Berlekamp E.R., "*Algebraic Coding Theory*", McGraw-Hill, New York, 1968.

[3] Bhargava V.K., Stein J.M., "*Configurations and Self-Dual Codes*", Inf. and Contr., vol. 28, pp. 352-355, Aug. 1975.

[4] Bose R.C., Chaudhari D.K. Ray, "*On a class of error correcting binary group codes*," Information and Control, vol. 3, no.1, pp. 68-79, 1960.

[5] Burton H.O., Weldon E.J., Jr.,"*Cyclic Product Codes*", Information Theory, IEEE Transactions on, IT-11, 433-439, 1965.

[6] Chen C.L., Peterson W.W., Weldon E.J., Jr., "*Some Results on Quasi-Cyclic Codes*", Inf. and Contr., vol. 15, pp. 407-423, 1969.

[7] Cohen A., "*Lower bounds on the error probability of a give binary block code*", Israel Institute of Technology, November 2002.

[8] Deza E., Deza M., "*Dictionary of Distances*", Elsevier, 2006.

[9] Elias P., "*Error-Free Coding*", IRE Transactions, PGIT-4, pp. 29-37, 1954.

[10] Gabidulin E., "*A brief survey of metrics in coding theory*", Mathematics of Distances and Applications, pp. 66-84, 2012.

[11] Gilbert E.N., "*A comparison of signalling alphabets*", Bell Syst. Tech. J., vol. 31, no. 3, pp. 504-522, 1952.

[12] Golay M.J., "*Notes on Digital Coding*", Proc. IRE, vol. 37, pp. 657-657, 1949.

[13] Hamming R.W., "*Error detecting and error correcting codes*", Bell System Technical Journal, vol. 29, no. 2, pp. 147-160, 1950.

[14] Hocquenghem A., "Codes correcteurs d' erreurs", Chiffres, vol. 2, pp. 147-156, 1959.

[15] Jain S., Nam K. B., Lee K. S., "*On some perfect codes with respect to Lee metric*",Linear algebra and its applications, 405, pp. 104-120, 2005.

[16] Karlin M., "*Decoding of Circulant Codes*", Information Theory, IEEE Transactions on, vol. IT-16, pp. 797-802, Nov. 1970.

[17] Karlin M., "*New Binary Coding Results by Circulants*", Information Theory, IEEE Transactions on, vol. IT-15, pp. 81-92, Jan. 1969.

[18] Kaushik M.L., "*A new metric in the study of error correcting codes*", Ph.D. Thesis,University of Delhi, 1979.

[19] McEliece R.J., "*The theory of information and coding*", Reading MA, Addison-Wesley, 1977.

[20] Lee C. Y., "*Some properties of nonbinary error-correcting codes*," Information Theory, IRE Transactions on, vol. 4, no. 2, pp. 77–82, 1958.

[21] Peterson W. W., Weldon E. J., Jr., "*Error-Correcting Codes*", 2nd ed., MIT Press, Cambridge, Mass., 1972.

[22] Peterson W.W., "*Binary coding of error control*", Proc. National Electronics Conference, vol. 16, pp. 15-21, 1960.

[23] Plotkin M., "*Binary codes with specific minimum distance*", Information Theory, IRE Transactions on, vol. 6, no. 4, pp. 445-450, Sept. 1960.

[24] Prang E., "*Cyclic error correcting codes in two symbols*", Air Force Cambridge Research Centre, Cambridge, Mass., vol. 57, no. 103, Sept. 1957.

[25] Reed I. S., Solomon G., "*Polynomial Codes Over Certain Finite Fields*", J. Soc. Ind. Appl. Math., vol. 8, pp. 300-304, June 1960.

[26] Shannon C. E., "*The mathematical theory of communication*", Bell System Technical Journal, vol. 27, pt. I, pp. 379-423, 1948; pt. II, pp. 623-656, 1948.

[27] Shannon C.E., Gallager R. G., Berlekamp E.R., "*Lower bounds to error probability for coding on discrete memoryless channels*", Information and Control, vol. 10, 65-103, 1967.

[28] Sharma B.D., Dial G., "*Some tighter bounds on code size with Sharma-Kaushik Metrics*", Presented at the Intern. Conf. on Math., Mao, Menorca, pp. 15-17, June 1987.

[29] Sharma B.D., Kaushik M. L., "*Algebra of Sharma and Kaushik's metric inducing partitions of Zq*", J. Combin. Information System Science Vol.11, pp. 19-32, 1986.

[30] Sharma B.D., Kaushik M. L., "*Error correcting codes through a new metric*", 41st Annual Conf. Intern. Stat. Inst., New Delhi, 1977.

[31] Sharma B.D., "*Partitioned Product of Matrices and Construction of Efficient Product Codes*", Jr. of Comb. Information & System Sciences, 33, 437-448, 2008.

[32] Sharma B.D., Kaushik M.L., "*Limited intensity random and burst error correcting codes with class weight consideration*", ElektronischeInformationsverarbeitung und Kybernetik, 15, pp. 315-321, 1979.

[33] Slepian D., "*Some further theory of group codes*", Bell System Technical Journal, 39, pp. 1219-1252, 1960.

[34] Tavares S. E., Bhargava V.K., Shiva S.G.S., "*Some rate p/(p+1) quasi-cyclic codes*", Information Theory, IEEE Transactions on, vol. IT-20, no.1, pp.133-135, Jan. 1974.

[35] Townsend R. L., Weldon E.J., Jr., "*Self-Orthogonal Quasi-Cyclic Codes*", Information Theory, IEEE Transactions on, vol. IT-13, pp. 183-195, Apr. 1967.

[36] Twitto M., "*Tightened upper bounds on the ML decoding error probability of binary linear block codes and applications*", Israel Institute of Technology, April 2006.

[37] Varshamov R.R., "*Estimate of the number of signals in error correcting codes*", Dokl. Akad. Nauk S.S.S.R., vol. 117, no. 5, pp. 739-741, 1957.

[38] Williams F.J., Sloane N.J.A., "*The theory of error correcting codes*", Amsterdam, Netherlands: North – Holland, 1977.

[39] Wolf J.K., "*On codes derivable from the tensor product of check matrices*", Information Theory, IEEE Transactions on, vol. 11, no. 2, pp. 281-284, 1965.

LIST OF PUBLICATIONS

(INTERNATIONAL REFERRED JOURNALS)

[1] **Gaur A.** and Sharma B.D., "Codes Correcting Limited Patterns of Random Error using SK-metric" Cybernetics and Information Technologies, vol.13, No. 1, 34-45, 2013.

Indexed in: INSPEC (The Database for Physics, Electronics and Computing), AMS Digital Mathematics Registry (American Mathematical Society), Elsevier SCOPUS, Microsoft Academic Search.

[2] **Gaur A.** and Sharma B. D., "*Upper Bound on Correcting Partial Random Errors*" Cybernetics and Information Technologies, vol.13, No. 3, 41-49, 2013.

Indexed in: INSPEC (The Database for Physics, Electronics and Computing), AMS Digital Mathematics Registry (American Mathematical Society), Elsevier SCOPUS, Microsoft Academic Search.

[3] **Gaur A.** and Sharma B. D., "*A Broad Class of Additive Error Coding, Channels and Lower Bound on the Probability of Error for Block Codes using SK-Metric*," International Journal of Applied Mathematics and Statistics, volume 52, Issue 1, 2014.

Indexed in: SCOPUS; Mathematical Reviews; Math Sci Net; Zentralblattfür Mathematik; ; ERA: Excellence in Research for Australia (by Govt. of Australia); Statistical Theory and Method Abstracts (STMA-Z), Current Index to Statistics (CIS) [The Current Index to Statistics (CIS) is a joint venture of the American Statistical Association & Institute of Mathematical Statistics, USA], International Abstracts in Operations Research (IAOR), Indian Science Abstracts; Academic keys; Journal Seek, Ulrich's Periodicals Directory, SCI mago Journal & Country Rank, International Statistical Institute (ISI, Netherlands) Journal Index, Index Copernicus.

[4] **Gaur A.** and Sharma B.D., "*A New Class of Cyclic Codes Using Ordered Power Product of Polynomials*", Journal of Applied Mathematics & Informatics, Vol.32, N0.3-4 (May, 2014)

Indexed in: Mathematical Reviews and Zentralblatt fur Mathematik

[5] **Gaur A.** and Sharma B. D. "*Perfect Codes Using Class Metric", International Journal of Research in Information Technology*", Volume 1, Issue 8, Pg. 81-90, August, 2013.

Indexed in: Google Scholar; Google; Yahoo; EntireWeb; AU Search Engine; Active Search Results – ASR; Smart Viper; Computer Science Directory; iSeek LIBRIS; New JOUR; Researchbib; GIF; ISRAJIF; JOUR Informatics; DRJI; Scientific Indexing Services (SIS).

Ankita Gaur
(Research Scholar)

Professor Bhu Dev Sharma
(Supervisor)