IOSR Journal of Mathematics (IOSR-JM)
ISSN: 2278-5728. Volume 4, Issue 6 (Jan. - Feb. 2013), PP 77-80
www.iosrjournals.org

Planar Near-Rings And Coding Theory

Anil Kumar Kashyap[1] and Madan Mohan Singh[2]
[1]*Chhatrapati Shivaji Institute of Technology,Durg (CG) INDIA*
[2]*Shri Shankaracharya College of Engineering and Technology,Bhilai (CG) INDIA*

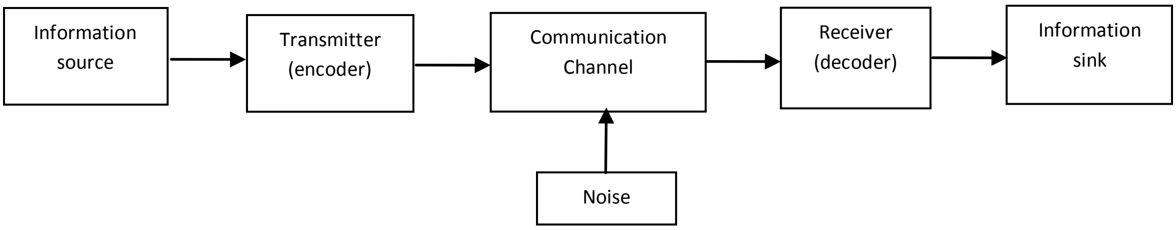
Abstract: *The purpose of this paper is to discuss the importance of algebraic coding theory and to investigate the special case in which BIB designs and codes are constructed from planar near-rings. Application of planar near-rings to binary codes were first explored by Modisett [12] and by Fuchs, Hofer and Pilz [14].*

Key word: *planar near-ring, incidence structure, tactical configuration, BIBD, binary codes, block code.*

I. Introduction:

Over the last 60 years, algebraic coding theory has become one of the most important and widely applied aspects of abstract algebra. Coding theory forms the basis of all modern communication systems, and is the key to another area of study, Information theory, which lies in the intersection of probability and coding theory. Algebraic codes are now used in essentially all hardware-level implementations of smart and intelligence machines, such as sensors, optical devices, telecom equipments. It is only with algebraic codes that we are able to communicate over long distances, or are able to achieve megabit bandwith over a wireless channel.

Algebraic coding is most prevalent in communication system, and has been developed and engineered because of one inescapable fact of communication: noise. Noise will always be a part of communication and has the potential to corrupt data and voice due to its presence. The following diagram provides a rough idea of a general information system:



The most important part of the diagram, as far as we are concerned, is the noise, for without it there would be no need for the theory.

Consider these basic applications of algebraic codes. Let us suppose that in the case of two warring nations, a message is to be sent indicating an intention of surrender or an intention of war. If a binary 1 is sent, the nation surrenders. If a binary 0 is sent, then war it is. In this time of such redundancy communication, there is the concept of noise or error correction, and so it is possible, if not likely that due to noise a transmitted 0 to be received as a 1, or vice-versa. To make this system substantially more robust, a party can transmit five bit and the receiver then infers a message based on the majority contents. For instance, if 00000 meant surrender and was sent, though due to a noise 00100 was received, the message remains intact and the white flag is raised. Based on the sender receiver agreement, up to three errors can occur before the message intent is reversed and ultimately lost. The probability of three bit error occurring can be shown to be lower than a single error and so the addition of this decoding makes the system more robust. This decision process is called the maximum likely hood decoding process.

Two main branches of coding theory are source coding and channel coding. They are so named because the former manipulates the source to allow more efficient transmission (i.e. small size message) while the latter addresses the errors that may be introduced in the transmission channel. The fundamental theorem of source coding was given by Claude Shannon [7] in 1948, widely considered the father of information theory. Shannon’s theorem describes the best possible error correction of a code given certain parameters. Source coding is more within the computer science and engineering discipline, with main applications being compression of data prior to transmission.

1. Definitions:

1.1. Word: A word is a sequence of digits.

1.2 Length of a word: The length of a word is the number of digits in the word.

1.3. Binary Code: A binary code is a set C of words. The code consisting of all words of length two is

$$C = \{00, 10, 01, 11\}$$

1.4. Block code: A block code is a code having all its words of the same length. The words that belong to a given code $C_{0,}$ will be called codewords. We shall denote the number of codewords in a code C by |C|.

1.5. Linear code: A (n,k) linear code over a finite field F is a k-dimensional subspace V of the vector space

$$F^n = \underbrace{F\oplus F\oplus F\oplus\ldots\ldots\ldots\oplus F}_{\text{(n tuples)}}$$

over F. The vectors $\alpha\in V$ are called the codewords. When $F = Z_2$, we refer to working with binary codes.

A (n, k) linear code over a finite field F can be thought of as a set of n-tuples from F , where each vectors contains both the message word and a redundancy , which are the remaining n-k components of the codeword. For any finite field of order q, there are their q^k possible codewords. In the common base of binary codes, for n digits, there are 2^n possible codewords. The set {0000, 0101, 1010, 1111} is a (q-2) binary code.

1.6. Hamming distance:

The Hamming distance between any two vectors $\alpha,\beta\in V$ is the number of components in when they differ . Let $d(\alpha,\beta)$denote the Hamming distance between any two vector α,β.

1.7. Hamming weight:

The Hamming weight of a vector $\alpha \in V$ is the number of non-zero components. The hamming weight of a linear code is the minimum weight of any non-zero vector in the code. Let $wt(\alpha)$ denote the Hamming weight of the vector α.

1.8. N*: [14]

If N is any set containing something like a "zero element" 0, N* will denote N \ {0}.

1.9. Block: [14]

Let N be a near-ring, $a \in N^*$ and $b\in N$. Then the aN + b is called a block determined by a, b. Blocks of the form aN ($a \neq 0$) are called basic blocks.

1.10. Incidence structure: [14]

Let P be a set and $\mathbf{B} \subseteq 2^P$. The **pair** (P, **B**) is called an incidence structure.

1.11 Tactical configuration: [14]

An incidence structure (P, **B**) ($\mathbf{B} \subseteq 2^P$) is said to be a tactical configuration with parameters (v, b, r, k) $\in$ N if

(i) |P| = v.

(ii) | **B** | = b.

(iii) Each $p \in P$ is in exactly r elements of **B.**

(iv) Each $B\in$ **B** contains exactly k elements of P, i.e. $\forall$ $B\in$ **B:** |B| = k.

1.12 Planar near-rings: [14]

A near-ring N is said to be a planar near-ring if $|N/\equiv| \geq 3$ and if every equation xa = xb + c has a unique solution (in N).

II. Planar Near-Rings and Balanced Incomplete Block Designs:

The study of how much experiment can be organized systematically so that statistical analysis can be applied is an interesting problem which is carried out by several researchers. In the planning of experiment it often occurs that results are influenced by phenomena outside the control of the experimenter. The introduction of balanced incomplete block design (BIBD) helps in avoiding undesirable influence in the experiment. In general, if we have to test the effect of r different conditions with m possibilities for each condition this leads to a set of r orthogonal latin squares.

A planar near-ring can be used to construct balanced incomplete block designs (BIBD) of high efficiency. In view of this we give the following definition.

2.1. Definition:

A balanced incomplete block design (BIBD) with parameters (ν , b, r, k, λ) is a pair (P, B) with the following properties:

(i) P is a set with ν elements,

(ii) $B = (B_{1,}\ldots\ldots\ldots,B_b)$ is a subset of p(P) with b elements,

(iii) Each B_i has exactly k elements where $k < \nu$,

Each unordered pair (p, q) with $p, q \in P$, $p \neq q$ occurs in exactly λ elements in B.

The set $B_1 ,.........,B_b$ are called the blocks of BIBD. Each $a \in P$ occurs in exactly r sets of B. Such a BIBD is also called a (ν, b, r, k, λ) configuration or 2 - (ν, k, λ) tactical configuration or design. The term balance indicates that each pair of elements occurs in exactly the same number of block, the term incomplete means that each block contains less than ν - elements. A BIBD is symmetric if ν = b.

The incidence matrix of a (ν, b, r, k, λ) configuration is the $\nu \times b$ matrix a = (a_{ij}) where

$$a_{ij} = \begin{cases} 1 & \text{if } i \in B_j \\ 0 & \text{otherwise.} \end{cases}$$

Here i denotes the i^{th} element of the configuration. The following conditions are necessary for the existence of a BIBD with parameters ν, b, r, k, λ.

1. $bk = r\,\nu$,
2. $r(k-1)= \lambda(\nu -1)$,
3. $b \geq \lambda$,

Recall that a near-ring N is called planar if for all equations $x \circ a = x \circ b + c$ ($a, b, c \in N$, $a \neq b$) have exactly one solution $x \in N$.

III. Planar Near-Rings and Coding theory:

Today a great deal of information is transmitted from point A to point B in the form of 0s and 1s. A sequence $a_1 a_2.........a_n$ of 0s and 1s represents a datum. If this sequence $a_1 a_2.........a_n$ leaves A, one hopes that the same sequence $a_1 a_2.........a_n$ arrives at B. But, it may be that $a_1 a_2.........a_n$ is transmitted from A and $b_1 b_2.........b_n$ is received at B, and $a_i \neq b_i$ for some i.

In transmitting a_i there is possibility that b_i is received, and $a_i \neq b_i$

As an example, suppose 0010101 represents the letter x. If 0010101 is sent from A and 1010101 is received at B, then there is an error in transmission. If 1010101 represent the letter y, then the recipient at B must assume that letter y was sent, even though, in truth, x was sent. In this example only one small error was made, but yet false information was received, and it was not detected.

How could the receiver at B (1) know that information had been received, and (2) correct the false information? An elementary example will quickly illustrate a possibility.

Suppose a communication system is designed to transmit exactly one of two values at a given time, a y for 'yes' and an n for 'no'. Suppose 11110000 represents y and 00001111 represents n. If one wants to transmit a y, then one transmits 11110000. But what if 11110001is received? Obviously an error has occurred and if only one error has occurred then interpreting 11110001 at B as 11110000 will correct the error. So error detection and error correction can take place. If the communication system is highly reliable, then one is reasonably assured that a received 11110001 was meant to be a 11110000. But suppose 11001010 was received at B. The receiver at B can not be confident of what was sent from A. Errors can be detected, but not necessarily corrected.

Certainly there are 2^n distinct sequences $a_1 a_2.........a_n$ of 0s and 1s. Perhaps this is significantly more than we need. For example, perhaps all we need are the 26 letters of the Roman alphabet, the 10 digits, 13 punctuation symbols, and one symbol for a blank. So, with a total of 50 symbols required, we take n=6 and with 2^6= 64, we have more than enough sequences $a_1 a_2.........a_n$ to represent the 50 symbol needed for effective communication. However, with n=10, we have 1024 such sequences $a_1 a_2.........a_{10}$. In order to detect and correct errors, we will want to isolate 50 of these 1024 sequences as much as possible.

Exactly what do we mean when we say 'we want to isolate' a sequence? Let a = $a_1 a_2.........a_n$ and b= $b_1 b_2.........b_n$ be two sequences of 0s and 1s of length n.

Define

$$d(a,b) = |\{i | 1 \leq i \leq n,\ a_i \neq b_i\}|$$

So d(a,b) counts the number of places where a differs from b , and so it is a measure of how much a differs from b. If a is transmitted from A and b is received at B, then d(a,b) errors have occurred. Let Z_2^n denote all sequences $a_1 a_2.........a_n$ of 0's and 1's. Then d is a metric on Z_2^n . That is for all $a,b,c \in Z_2^n$,

(i) d(a,b) = d(b,a),

(ii) $d(a,c) \leq d(a,b) + d(b,c)$,

(iii) d(a,a) = 0 and

(iv) if d(a,b) = 0,than a = b.

To see that d is a metric on Z_2^n is immediate except for (ii). Suppose a and b differ at $i_1, i_2, \ldots, i_k$, so d(a,b) = k. Suppose b and c differ at $j_1, j_2, \ldots, j_l$, so d(b,c) = *l*.

Also suppose a and c differ at $s_1, s_2, \ldots, s_m$, so d(a,c)= m. If $a_s \neq c_s$, than we can not have both $a_s = b_s$ and $b_s = c_s$. So $s \in \{ i_1, i_2, \ldots, i_k \}$ or $s \in \{ j_1, j_2, \ldots, j_l \}$ or $s \in \{ i_1, i_2, \ldots, i_k \} \cap \{ j_1, j_2, \ldots, j_l \}$. Hence m $\leq$ k+*l* or d(a,c) $\leq$ d(a,b) + d(b,c). If $a_1, a_2, \ldots, a_M$ are M of the 2^n distinct sequences $a_1, a_2, \ldots, a_n$ of 0's and 1's, then we want a positive r so that if $1 \leq d(b,a_i) \leq r$, then $b \notin \{ a_1, \ldots, a_n \} \setminus \{ a_i \}$ for each i, $1 \leq i \leq M$. Thus $a_1, a_2, \ldots, a_M$ are "isolated". We will return to this idea shortly.

Let C(n) denote a non-empty set of sequences a= $a_1 a_2 a_3 \ldots a_n$ of 0s and 1s where n is a positive integer measuring the length of the sequence. So $1 \leq |C(n)| \leq 2^n$. If a, $b \in C(n)$ and $a \neq b$ then $1 \leq d(a,b) \leq n$, and so

$$D = \min \{d(a,b) \in C(n), a \neq b\} \text{ exists}$$

and we are assured that $1 \leq D \leq n$. If M = |C(n)|, then we refer to C(n) as an (n, m, D) - (binary) code. Our code will be binary in that each element of C(n) is a sequence of 0s and 1s . There is function $w:C(n) \rightarrow \{0,1,\ldots,n\}$ defined by $w(a_1 a_2 \ldots a_n) = |\{i | 1 \leq i \leq n, a_i = 1\}|$. So $w(a_1 a_2 \ldots a_n)$ is the weight of the codeword a= $a_1 a_2 \ldots a_n \in C(n)$. Of all the possible codes C(n), some have advantages over others. When one has a finite tactical configuration (N, B, $\in$), one can easily construct two codes, a row code $C^A(\nu)$ and column code $C_A(b)$. Following the conventions in MacWilliam and Sloane [M&S] [13], we define for a finite tactical configuration (N, B, $\in$) an incidence matrix A, a $b \times \nu$ matrix of 0s and 1s. Let B= $(B_1, B_2, \ldots, B_b)$ and N=$(x_1, x_2, \ldots, x_\nu)$.

Define

$$A = (a_{ij}) \text{ where } \qquad a_{ij} = \begin{cases} 1 & \text{if } x_j \in B_i \\ 0 & \text{otherwise.} \end{cases}$$

Let $C^A(\nu)$ consist of the codewords $a_1, a_2, \ldots, a_b$ where $a_i = a_{i1}, a_{i2}, \ldots, a_{i\nu}$. Let $C_A(b)$ consist of the distinct codewords $b_1, b_2, \ldots, b_\nu$, where $b_j = a_{1j}, a_{2j}, \ldots, a_{bj}$. That is, $C^A(\nu)$ consists of the b-rows of A and $C_A(b)$ consists of the distinct columns from the ν columns of A. Then $C^A(\nu)$ is a (ν, b, D_ν) - code for some, D_ν and $C_A(b)$ is a (b, ν', D_b) -code for some $\nu', 1 \leq \nu' \leq \nu$. Actually, any (n, M, D)-binary code C(n) has several incidence matrices A. Let C(n)= $\{ a_1, a_2, \ldots, a_M \}$ with $a_i = a_{i1}, a_{i2}, \ldots, a_{in}$, and then let A = (a_{ij}). Now $C^A(n)$ = C(n) and $C_A(M)$ are as before. If one takes any s × t matrix A = $\{a_{ij}\}$, where each $a_{ij} \in \{0,1\}$, then let $C^A(t)$ consists of the distinct rows of A and let $C_A(s)$ consists of distinct columns of A. So $C^A(t)$ and $C_A(s)$ are binary codes.

The codes $C^A(\nu)$ and $C_A(b)$ are nice in that they are constant weight codes. A code C(n) is a constant weight code if there is a number W so that w(a) = W for each $a \in C(n)$. Hence W = K for $C^A(\nu)$ and w = r for $C_A(b)$. This is because each block $B \in \mathbf{B}$ has exactly k elements and each $x \in N$ belongs to exactly r blocks.

References:

[1] Aichinger, E.: "Planar rings", Results in Mathematics 30 (1996), 10–15.

[2] Abbasi, S.J. and Iqbal, K. : "On Units in Near Rings", TECHNOLOGY FORCES (Technol. forces): PAF-KIET Journal of Engineering and Sciences Volume 02, Number 01, January- June 2008.

[3] Beidar, K. I., Fong, Yuen, and KE, Wen Fong "On finite circular planar near-rings", J. Algebra 85 (1996), 688–709.

[4] Blake, I. F. and Mullin, R. C.: "The Mathematical Theory of Coding", New York: Academic, 1975.

[5] Clay, J. R.: "Generating balanced incomplete block designs from planar near-rings", J. Algebra 22 (1972), 319–331.

[6] Clay, J. R.: "Generating balanced incomplete block designs from planar nearrings", Oberwolfach, 1972.

[7] Claude Shannon: "The Mathematical Theory of Communications", Bell system,Technical journal,1948.

[8] Clay, J. R.: "Near-ring: Geneses and application", Oxford Univ. Press Inc. Oxford, 1992.

[9] Eggetsberger, Roland: "Codes from some residue class ring generated finite planar near-rings",Institutsber. No. 467,1993, Univ. Linz, Austria.

[10] Ferrero, G.:"Stems planari e BIB - disegni", Riv. Mat, Univ, Panna., Vol.11, pp 79-96, 1970.

[11] Fuchs, Peter R., Hofer, Gerhard, and Pilz, Günter: "Codes from planar near-rings", IEEE Trans. on Information Theory 36 (1990), 647-651.

[12] Modisett, M.C.: "A characterization of the circularity of balanced incomplete block designs", Utilitas Math, vol. 35, pp 83-94, 1989.

[13] Mac Williams, F.J. and Salone, N. J.: "The Theory of Error Correcting Codes-I , II", Amsterdom: North Holland, 1977.

[14] Pilz, G.: "Near-rings". North Holland and / American Elsevier, Amsterdam, Second, revised edition.1983.