International Journal of Mathematical Engineering and Science
ISSN : 2277-6982 Volume 3 Issue 1 (January 2014)
http://www.ijmes.com/ https://sites.google.com/site/ijmesjournal/

An algorithm to construct error correcting codes from planar near-rings

Abdelkarim Boua[1,1], Lahcen Oukhtite[1],
Abderrahmane Raji[1] and Omar Ait Zemzami[2],

[1] Moulay Ismail University, Faculty of Sciences and Technics
Department of Mathematics, Group of Algebra and Applications
PO. Box 509 Boutalamine, Errachidia, Morocco
E-mail: karimoun2006@yahoo.fr, oukhtitel@hotmail.com,
rajiabd2@gmail.com

[2] Moulay Ismail University, Faculty of Sciences and Technics
Computer Science Department
PO. Box 509 Boutalamine, Errachidia, Morocco
E-mail: omarzemzami@yahoo.fr

Abstract. The purpose of this paper is to indicate the importance of using the planar near-rings in the construction of the Balanced Incomplete Block Designs (BIBD) of high efficiency, and how the latter can be used for constructing and developing error correcting codes. Consequently, an algorithm of a program to calculate the incidence matrix and the error correcting codes from a planar near-ring will be drawn.

Keywords: Planar near-ring, BIBD, Error correcting code.

1 Introduction and Motivation

Near-rings are one of the generalized structures of rings. The study and research on near-rings is very systematic and continuous. Near-ring have been used since the development of calculus, but the key idea behind near-rings was formalized in 1905 by Dickson who defined the near-fields. Veblin and Wedderburn used Dickson's near-field to give examples of Nondesarguesian planes. In late 1930s, Wieland studied near-rings, which were not near-fields. Extensive studies about the subject can be found in two famous books on near-rings [6] and [7]. Near-rings abound in all directions of mathematics and continuous research is being conducted, which shows that their structure has power and beauty in all its own. Importantly, the study of the

[1,1] The corresponding author.

theory of planar near-rings has received momentum in the last decades. Various applications of planar near-rings have been applied in different fields (see for example [3], [6]). Indeed, the considerable development of the theory of planar near-rings in the last decade has been largely due to its strong links with the theory of experimental designs, combinatory (see for example [1], [2]) as well as applications of in various fields such as group theory geometry and its branches, combinations, design of statistical experiments, coding theory and cryptography, and particularly in error codes correcting (see for example [5]). The planar near-rings theory is also used in the construction of balanced incomplete block designs (BIBD) of high efficiency, as well as in the improvement of error correcting codes.

2 Definitions and terminology

Recall that a right (resp. left) near-ring is a set N together with two binary operations '+' and '·' such that

(i) $(N,\ +)$ is a group (not necessarily abelian).

(ii) $(N,\ .)$ is a semigroup.

(iii) For all $x, y, z \in N,\ (x+y).z = x.z + y.z\ (resp\ \ x.(y+z) = x.y + x.z).$

Now we remind some definitions and properties of near-rings, for details see [3].

Definition 1. For a near-ring $(N,+,.)$ and $a,\ b \in N$, define an equivalence relation $:$ on N by $a : b$ if and only if $xa + xb$ for all $x \in N$. If $a : b$, we say that a and b are equivalent multipliers.

Definition 2. A near-ring $(N,+,.)$ is said to be planar if:

(i) $:$ has at least three equivalence classes, i.e, $|N/:| \geq 3.$

(ii) For constants $a,b,c \in N$ where a is not equivalent to b , the equation $x.a = x.b + c$ has a unique solution for $x \in N.$

Example 1. Let $N = (\mathrm{Z}_5,+,*)$ where + is the standard addition + and $*$ is defined by: $n*0 = 0,\ n*1 = n*2 = n,\ n*3 = n*4 = 4n$ for all $n \in \mathrm{N}$. Then $1 : 2$ and $3 : 4$ so that $|N/:| \geq 3$. Moreover, as 2 is not equivalent to 3 and the equation $x*2 = x*3+1$ has a unique solution $x = 3$, it follows that N is planar near-ring.

Definition 3. A balanced incomplete block design $\left(\text{BIBD}\right)$ with parameters (v, b, r, k, λ) is a pair (P, B) with the following properties:

(i) P is a set with v elements.

(ii) $B=\{B_1, ..., B_b\}$ is a subset of P with b elements are called the blocks a (BIBD).

(iii) Each B_i has exactly k elements where $k < v$ each unordered pair (p, q) with $p, q \in P$, $p \neq q$ occurs in exactly λ elements in B.

Each $a \in P$ occurs in exactly r sets of B. 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 v elements.

The main parameters of a $\left(\text{BIBD}\right)$ are (v, b, r, k, λ) and the parameters satisfy the following necessary conditions for existence.

$$\begin{aligned} vr &= kb, \\ \lambda(v-1) &= r(k-1). \end{aligned}$$

There are good construction methods for obtaining planar near-rings. We exhibit the following one, due to J. R. Clay ([1], [2], [3], [4]), which is both easy and most useful.

Theorem 1. Let F be a field of order p^n, where p is a prime and let t be a nontrivial divisor of p^n-1, so $st = p^n -1$ for some s. Choose a generator g of the multiplicative group of F. Define $g^a \cdot_t g^b := g^{a+b-[b]_s}$, where $[b]_s$ denotes the residue class of a modulo s. Then $N = (F, +, \cdot_t)$ is a planar near-ring with $N^* = N \setminus \{0\}$.

3 Construction of (BIBD) from planar near-rings

A planar near-ring can be used to construct $\left(\text{BIBD}\right)$ of high efficiency where by high efficiency "E" we mean $E = \dfrac{\lambda v}{rk}$, this E is a number between 0 and 1 and it estimates the quality of any statistical analysis if $E \geq 0,75$ the quality is good.

According to [2], the construction of a $\left(\text{BIBD}\right)$ from a planar near-ring can be obtained as follows:

Theorem 2.
Let N be a finite planar near-ring and $B = \left\{aN^* + b \mid a,\ b \in N,\ a \neq 0\right\}$, then $(N\ ,\ B)$ is a $\left(\text{BIBD}\right)$ with parameters $(v,\ \dfrac{v(v-1)}{k}, v-1,\ k,\ k-1)$ where $v = \left|N\right|$ and k is the cardinality of each aN^* with $a \neq 0$.

It is often convenient to represent a (BIBD) by means of an incidence matrix. This is especially useful for computer programs. Here we recall the definition of an incidence matrix.

Definition 4. Let (P, B) be a (BIBD) where $P = \left\{p_1, \ldots.., p_v\right\}$ and $B = \left\{B_1, \ldots.., B_b\right\}$. The incidence matrix of (P, B) is the $v \times b$ matrix $M = (m_{ij})$ defined by the rule

$$m_{ij} = \begin{cases} 1 \ , \text{ if } \ p_i \in B_j \\ 0 \ , \text{ otherwise.} \end{cases}$$

The incidence matrix M of a (v, b, r, k, λ)-BIBD satisfies the following properties:

$i)$ every column of M contains exactly k "1" s.

$ii)$ every row if M contains exactly r "1" s.

$iii)$ two distinct rows of M both contain "1" s in exactly λ columns.

Our aim in the following example is to construct a (BIBD) and its incidence matrix.

Example 2. Let $N = (\mathrm{Z}_5\ ,+,\ ._2)$ where '$+$'and '$._2$' are defined by:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

$\cdot_2$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	1	4	4
2	0	2	2	3	3
3	0	3	3	2	2
4	0	4	4	1	1

It is easy to check that N is a planar near-ring. In the multiplication table above we observe that

$$1\cdot_2 Z_5^* = 4\cdot_2 Z_5^* \quad \text{and} \quad 2\cdot_2 Z_5^* = 3\cdot_2 Z_5^*$$

Then the blocks given by the relation $a\cdot_2 Z_5^* + b \ (a \neq 0)$ are:

$B_1 = 1\cdot_2 Z_5^* + 0 = \{1,4\}$, $B_2 = 1\cdot_2 Z_5^* + 1 = \{2,0\}$, $B_3 = 1\cdot_2 Z_5^* + 2 = \{3,1\}$, $B_4 = 1\cdot_2 Z_5^* + 3 = \{4,2\}$, $B_5 = 1\cdot_2 Z_5^* + 4 = \{0,3\}$, $B_6 = 2\cdot_2 Z_5^* + 0 = \{2,3\}$, $B_7 = 2\cdot_2 Z_5^* + 1 = \{3,4\}$, $B_8 = 2\cdot_2 Z_5^* + 2 = \{4,0\}$, $B_9 = 2\cdot_2 Z_5^* + 3 = \{0,1\}$, $B_{10} = 2\cdot_2 Z_5^* + 4 = \{1,2\}$.

Then (N,B) is a (BIBD) with the parameters $(v,\ b,\ r,\ k,\ \lambda) = (5,10,4,2,1)$. The incidence matrix of this design is the following 5×10 incidence matrix:

$$M_B = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

4 Construction of error correcting codes from (BIBD)

The main goal of coding theory is the following: given some alphabet A, a message over A is a word $a_1a_2....a_k$ of length k. If this transmitted over a "long" channel, error might occur at the receiver's end. In order to detect and correct these messages, they will be encoded (= prolonged) to $a_1a_2....a_ka_{k+1}....a_n$ before transmission. The test symbols $a_{k+1}....a_n$ are to be computed in some way from $a_1,.....,a_k$ so that, for each other message $b_1.....b_n$, the resulting codewords $a_1....a_n$ and $b_1....b_n$ are distinct, in this way, a small number of errors can be detected and even corrected. The Hamming distance $d(a_1....a_n, b_1....b_n)$ of two codewords is the number of places i in which a_i and b_i differ. The Hamming weight $wt(a_1....a_n)$ of $a_1....a_n$ is the number of places i where $a_i \neq 0$ (if $0 \in \mathrm{A}$). A code C of length n is a set of codewords of length n, its minimal distance drain (C) is the minimal distance between two different codewords. If $d = d_{\min}(C)$ then up to $d-1$ errors can be detected and up to $\left[\frac{d-1}{2}\right]$ errors can even be corrected. Of course, one wants $n-k$ to be small and d to be large. These are contradicting goals, and one seeks "optimal compromises". If A is a field and C a subspace of A^n then C is called a linear code. If $A = Z_2$, then C is called a binary code. All our codes will be binary; for more on codes see, e.g.,[8].

Now using the planar near-rings one can construct error correcting codes from BIBD).

Indeed, by taking either the rows or columns of the incidence matrix of such a (BIBD) one can obtain error correcting codes with several features.

Theorem 3 ([5]). The rows and the columns of the incidence matrix can both be viewed as a binary code, called the row code C_{rowB} (column code C_{colB}, respectively) of B.

Proposition 1 ([5]). Let the notation be as in definition 4.

a) C_{rowB} has v codewords of length b, equal weight r and minimal distance $2(r-\lambda)$.

b) C_{colB} has b codewords of length v, equal weight k and minimal distance $(k-m)$, where $m=\max_{i\neq j}\left|B_i \cap B_j\right|$.

c) Neither C_{rowB} nor C_{colB} can be linear.

Example 3. From the incidence matrix of example 2, we can extract a row code with 5 codewords and each codewords is a row of the incidence matrix of length 10, weight 4 and minimum distance is 6. Similarly, we can extract a column code with 10 codewords, and each codewords represents a column of the incidence matrix of length 5, and its weight 2 and minimum distance is 1. Hence the row code can detect 5 errors and correct 2 errors, and the column code doesn't detect and doesn't correct any errors. In this example, we conclude that the row is more efficient than the column code.

Now, our main result is to find an algorithm to construct error correcting codes from planar near-rings. It also determines the number of errors which can be detected by these codes and the number of possible corrections for each code. For this, it suffices to find the incidence matrix of planar near-rings. It should be noted that the proposed algorithm will be based on Theorem 1 and Theorem 2.

Algorithm.

```
Input: $m$ integer number
Output: an incidence matrix.
If $m = p^n$, then
1. Define a field $F$ of order $p^n$.
$i)$ $t$: divisor of $p^n - 1$ such that $st = p^n - 1$.
$ii)$ $g$: multiplicative generator of $F$.
```

2. Define law ‘ $\cdot_t$ ’ Such that: $g^a \cdot_t g^b := g^{a+b-[b]_s}$, where $[b]_s$ denotes the residue class of b modulo s. Then $N=(F,+,\ \cdot_t)$ is a planar near-ring.

3. The construction of BIBD.

```
    a)  $B=\{\alpha N^* + \beta \mid \alpha,\beta \in N,\ \alpha \neq 0\}$.
    b)  $v \leftarrow card(N)$
        $k \leftarrow card(\alpha N^*)$
        $b \leftarrow \frac{v(v-1)}{k}$
        $r \leftarrow v-1$
        $\lambda \leftarrow k-1$
```

(v,b,r,k,λ) parameters of (BIBD) - (N,B).

4. The construction of incidence matrix.

```
   For $i=1:v$
      For $j=1:b$
            $m_{ij} = \begin{cases} 1 \text{ , if } n_i \in B_j \text{ where } n_i \in N \text{ and } B_j \in B \\ 0 \text{ , else.} \end{cases}$
      end For.
   end For.
```

```
else

► Decompose $m$ into prime factors
► Initialize $m = p^n$ where $p$ is the largest prime factors in the decomposition.
► Return to step 1.

end If.
```

Example 4. If you use the program of this algorithm by taking $p=11$, then $t=2$, $s=5$ and $g=2$. Moreover, we find the following results: the incidence matrix is of order 11×22 contains only 0 and 1:

$$m_{inc} = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}$$

The incidence matrix of this example, we extract a row code with 11 codewords and each codewords is row of the incidence matrix of length 22, weight 10 and minimum distance is 12. Similarly, we extract a column code with 22 codewords , and each codewords represents a column of the incidence matrix of length 11, and its weight 5 and minimum distance is 2. Hence the row code can detect 11 errors and correct 5 errors, and the column code can detect a single error but it doesn't correct any error. On the other hand we found that the effectiveness of this (BIBD), $E = 0.88 \geq 0.75$, thus indicating that its quality is good.

References

1. J. R. Clay, Generating balanced incomplete block designs from planar near-rings, J. Algebra, 22, 319-331 (1972).
2. J. R. Clay, Geometric and combinatorial ideas related to circular planar near-rings, Bulletin of the Institute of Mathematics Academia Sinica, 16, 275-283 (1988).
3. J. R. Clay, Near-rings: Geneses and Applications, Oxford University Press, 1992.
4. J. R. Clay, Geometry in fields, Algebra Colloq., 1, n^{o} 4, 289-306 (1994).
5. P. Fuchs, G. Hofer and G. Pilz, Codes from planar near-rings, IEEE Trans. Inform. Theory, 36, 647-651 (1990).
6. G. Pilz, Near-rings, North Holland and American Elsevier, Amsterdam, Second revised edition (1983).

7. J. D. P. Meldrum, Near-rings and their links with groups, Research Notes in Mathematics Series, Pitmann. London, 3-10 (1985).
8. C. J. Maxson and G. Pilz, Endomorphisms of fibered groups, Proc. Edinburgh Math. Soc. (2) 32, n^o 1, 127-129 (1989).