PBIBDs from weakly divisible nearrings and related codes

Anna Benini

Abstract

In [5] the authors are able to give a method for the construction of a family of partially balanced incomplete block designs from a special class of wd-nearrings (*wd-designs*). In this paper the wd-design incidence matrix and the connected row and column codes are studied. The parameters of two special classes of wd-designs and those of the related row and column codes are calculated.

1 Introduction

In [10] a general method to construct partially balanced incomplete block designs on the set X is given, starting from a transitive permutation group H on X with an intransitive subgroup S.

Obviously, from such a general method no formulae arise for the design parameters computation. A possible way to obtain the computability of the parameters is to link the action of H to the action of some operation defined on X, making X an algebraic structure. This could be an efficient tool to work with. Following such a line, in [5], a class of partially balanced incomplete block designs (wd-designs) is constructed and formulae for their parameters are found.

In this paper the incidence matrix of the above designs and the related row and column codes are studied. In more detail:

In Section 2 the basic definitions related to *partially balanced incomplete block designs* ($PBIBD$s) can be found and a frame of the whole construction, based on [3, 4, 5], is given.

In Section 3 the incidence matrix of the constructed $PBIBD$s is studied.

In Section 4 the parameters of the row and column codes related to the above incidence matrix are found.

In Section 5 two special classes of $PBIBD$s are considered, for which all the parameters can be easily calculated.

2 Partially Balanced Incomplete Block Designs

A *Partially Balanced Incomplete Block Design* is a complex structure: a *block design* and an *association scheme* are defined together on the same set and they fit. We give the basic definitions here.

[0]MSC: primary 05B05, secondary 05E30, 94B25

Keywords : block designs, association schemes, cyclic codes

Work carried out on behalf of Italian M.I.U.R.

Definition 2.1 An incidence structure $(X, \mathcal{B} \subseteq \mathcal{P}(X))$ is called *block design* (or *tactical configuration*) if all the blocks have the same size k and all the elements have the same replication number r, which means they occur in the same number r of blocks. A block design is said to be *incomplete* (IB-design) if at least one of its blocks is a proper subset of X. The numbers (v, b, r, k), where v and b are the cardinality of X and $\mathcal{B}$ respectively, are called the *parameters* of the design. We know that they are not independent, because $vr = bk$ holds.

For more information on design theory we refer to [7].

Definition 2.2 An *association scheme with m associate classes* on a finite set X is a family of m symmetric and antireflexive binary relations $R_1, \ldots, R_m$ on X such that:

(i) any two distinct elements of X are ith associates for exactly one value of $i = 1, \ldots, m$;

(ii) for all $i = 1, \ldots, m$ and $x \in X$, there are exactly n_i distinct elements $y \in X$ so that $(x, y) \in R_i$;

(iii) for all $i, j, k = 1, \ldots, m$, if $(x, y) \in R_k$, the number p_{ij}^k of $z \in X$ so that $(x, z) \in R_i$ and $(y, z) \in R_j$ is a constant depending on i, j, k but not on the particular choice of x and y.

For further information about association schemes see [2].

Definition 2.3 A tactical configuration $(X, \mathcal{B})$ with an association scheme on X is called *partially balanced incomplete block design* ($PBIBD$) if there are positive integers λ_i, $i = 1, \ldots, m$, such that, if $x, y \in X$ are any two ith associate elements, then x, y occur together in exactly λ_i blocks of $\mathcal{B}$.

Thus a $PBIBD$ has the tactical configuration parameters v, b, r and k, the association scheme parameters n_i and p_{ij}^k, and the partial balance parameters λ_i, in addition. We refer to [13] for more information on $PBIBD$s.

2.1 $PBIBD$s from wd-nearrings

A *left nearring* is an algebraic structure $N = (S, +, *)$ such that $(S, +)$ is an additive group, $(S, *)$ is a multiplicative semigroup, and the left distributive low holds (see [8, 14]). A weakly divisible nearring (*wd-nearring*) is a left nearring N in which at least one of the equations $ax = b$ or $bx = a$ has a solution in N, for all $a, b \in N$ (see [6]).

From [3, 4], we know that a class of wd-nearrings is constructible starting from a pair (G, Φ), where G is the abelian group $(\mathbb{Z}_{p^n}, +)$ and Φ is a proper non trivial subgroup of $Aut(G)$, and giving a rule for a multiplication " $*$ " on $(\mathbb{Z}_{p^n}, +)$ which makes $(\mathbb{Z}_{p^n}, +, *)$ a wd-nearring. In [5], starting from the wd-nearrings of [3, 4], a family of $PBIBD$s (*wd-designs* in the sequel) is constructed when p is odd. As we are interested in the above wd-designs, in the following paragraph we summarize the main steps of the construction given in [3, 4, 5].

2.1.1 Construction

First step. Consider the additive group $G = (\mathbb{Z}_{p^n}, +)$, $n > 1$ and p prime odd, and choose Φ, a proper non trivial subgroup of $Aut(G)$ of order tp^h, $(t, p) = 1$. Set $Q = p\mathbb{Z}_{p^n}$ and $C = \mathbb{Z}_{p^n} \setminus Q$, so $N = C \cup Q$ and $C \cap Q = \emptyset$.

Select a set E of the representatives e_x of the Φ-orbits covering C in such a way that " if $e_a - e_b \notin p^j\mathbb{Z}_{p^n}$, $(j < n)$, then $x - y \notin p^j\mathbb{Z}_{p^n}, \forall x \in \Phi(a), \forall y \in \Phi(b)$ ". Fix e among the elements of E and

define[1]:

$$a * b = \begin{cases} 0 & if\ a = 0 \\ bp^r \phi_{ke^r}(e^{-r}) & if\ a = kp^r \text{ with } k \in \mathbb{Z},\ (k,p) = 1 \text{ and } 0 \leq r < n \end{cases}$$

Then $N = (Z_{p^n}, +, *)$ *results in a wd-nearring.*

Second step. Now, both the nearring multiplication " $*$ " and the usual ring multiplication (no symbol) are defined on $\mathbb{Z}_{p^n}$. Obviously $a * b = b(a * 1)$, for all $a, b \in \mathbb{Z}_{p^n}$. In the sequel, without loss of generality, we can set $e = 1$. Thus we obtain $N * 1 = \{0\} \cup \Phi(1) \cup \Phi(p) \cup \cdots \cup \Phi(p^{n-1})$ and we deduce $N * a = a(N * 1)$.

In this way *cyclic wd-designs can be generated*:

orbital wd-designs $\mathcal{D}_a = (N, \mathcal{B}_a)$, where a is a fixed element of C and $\mathcal{B}_a = \{N * a + b \mid b \in N)\}$. We obtain $c = p^{n-h-1}(p-1)/t$ orbital wd-designs, isomorphic to each other;

the *union wd-design* $\mathcal{D} = (N, \mathcal{B})$, where $\mathcal{B} = \{N * a + b \mid a \in C, b \in N\} = \bigcup_{a \in C} \mathcal{B}_a$. It is the union of the previous ones.

Third step. Consider the Φ-orbit Δ_i and set $U_i = \Delta_i \cup (-\Delta_i)$. If $\Delta_i = -\Delta_i$, we say that Δ_i is *self-paired* and in this case $U_i = \Delta_i$. If Δ_i is not self-paired, then $\Delta_i \cap (-\Delta_i)$ is empty. Anyway we define x and y to be ith associates if $x - y$ belongs to U_i. In this way *an association scheme is given on* $(Z_{p^n}, +)$. It fits with the previously constructed block designs and we obtain $PBIBD$s.

2.1.2 Notations and parameters

In the sequel, to remember easily and quickly the main definitions and properties from [3, 4, 5], the following keys could be useful.

notations		
Φ	automorphism group of $(\mathbb{Z}_{p^n}, +)$	$1 < \lvert\Phi\rvert = tp^h < (p-1)p^{n-1}$ $(t,p) = 1$
$N =$ $(\mathbb{Z}_{p^n}, +, *)$	constructed wd-nearring	$N = C \cup Q$ $Q = p\mathbb{Z}_{p^n}$, $C = N \setminus Q$
f	number of the non trivial Φ-orbits	$= \dfrac{(ph - h + p)p^{n-h-1} - 1}{t}$
c	number of the Φ-orbits in C	$= \dfrac{p-1}{t} p^{n-h-1}$
$E = (e_j)$	representatives of the Φ-orbits in C	$j = 1, \ldots, c$
Δ_l	lth non trivial Φ-orbit	$l = 1, \ldots, f$
$\Delta_i, -\Delta_i$	paired Φ-orbits	$\lvert\Phi\rvert$ even : self-paired $\lvert\Phi\rvert$ odd : not self-paired
$U_i =$ $\Delta_i \cup (-\Delta_i)$	union set of paired Φ-orbits	$i = 1, \ldots, m$ where $m = f$ if $\lvert\Phi\rvert$ is even $m = f/2$ if $\lvert\Phi\rvert$ is odd
$D = (d_i)$	representatives of the U_i	$i = 1, \ldots, m$
$B_{a,b}$	block generated by $a \in C$ and $b \in N$	$B_{a,b} = N * a + b$
$[B_{a_1,b_1} - B_{a_2,b_2}]$	list of differences between the elements of B_{a_1,b_1} and those of B_{a_2,b_2}	
$f_{a_1,a_2,k}$	frequency of k in $[B_{a_1,0} - B_{a_2,0}]$	in particular $f_{a,a,k} = f_{a,k}$
$\mathcal{D}_a = (N, \mathcal{B}_a)$	orbital wd-design	a fixed element of C $\mathcal{B}_a = \{B_{a,b} \mid b \in N)\}$
$\mathcal{D} = (N, \mathcal{B})$	union wd-design	$\mathcal{B} = \bigcup_{a \in C} \mathcal{B}_a =$ $\{B_{a,b} \mid a \in C, b \in N\}$

[1] We recall that ϕ_x denotes the automorphism of Φ such that $\phi_x(e_x) = x$, where e_x is the selected representative of the orbit $\Phi(x)$.

parameters					
association scheme					
$x, y \in \mathcal{R}_i$	ith associate elements			if $x - y \in U_i$	
m	number of the associate classes			$m = f$ if $\lvert\Phi\rvert$ is even $m = f/2$ if $\lvert\Phi\rvert$ is odd	
n_i	number of the ith associates elements			$n_i = \lvert\Delta_i\rvert$ if $\lvert\Phi\rvert$ is even $n_i = 2\lvert\Delta_i\rvert$ if $\lvert\Phi\rvert$ is odd	
p_{ij}^k	number of the ith associates of x and jth associates of y when x and y are kth associates				
	tactical configuration				partial balance
design	v	b	k	r	λ_i
$\mathcal{D}_a = (N, \mathcal{B}_a)$	p^n	p^n	$\frac{p^{h+1}-1}{p-1}t + (n-h-1)t + 1$	k	$(\lambda_i)_a = f_{a,d_i} = f_{1,d_i a^{-1}}$
$\mathcal{D} = (N, \mathcal{B})$	p^n	cp^n	$\frac{p^{h+1}-1}{p-1}t + (n-h-1)t + 1$	ck	$\lambda_i = \sum_{e_j \in E} f_{1,d_i e_j}$

Propositions 4.1 and 4.2 of [5] show that, for any $k \in N$,

$$f_{a_1,a_2,k} = f_{a_1,a_2,\phi(k)} \ \forall \phi \in \Phi, \quad \forall a_1, a_2 \in C \quad \text{and} \quad f_{a,k} = f_{1,ka^{-1}}, \ \forall a \in C$$

Thus, to know the frequency of k in the list $[B_{a_1,0} - B_{a_2,0}]$ it is sufficient to know the frequency of any element of its orbit $\Phi(k)$ in the same list. Moreover, for any $a \in C$, the frequency of k in $[B_{a,0} - B_{a,0}]$ equals the frequency of ka^{-1} in $[B_{1,0} - B_{1,0}]$.

Previous results can be generalized by the following statements, in order to give some information about the cardinality of the block intersection.

Proposition 2.4 *Let B_{a_1,b_1} and B_{a_2,b_2} be two blocks of the wd-design $\mathcal{D} = (N, \mathcal{B})$. Set $a = a_2 a_1^{-1}$ and $k = (b_2 - b_1)a_1^{-1}$. Then*

$$|B_{a_1,b_1} \cap B_{a_2,b_2}| = f_{1,a,k}$$

Let $y \in B_{a_1,b_1} \cap B_{a_2,b_2}$. Then there are $x, \overline{x} \in N$ so that $y = x * a_1 + b_1 = \overline{x} * a_2 + b_2$. Setting $a = a_2 a_1^{-1}$ and $k = (b_2 - b_1)a_1^{-1}$, we obtain $x * 1 - \overline{x} * a = k$, thus $k \in [B_{1,0} - B_{a,0}]$. Suppose that $y' = x' * a_1 + b_1 = \overline{x}' * a_2 + b_2$ belongs to $B_{a_1,b_1} \cap B_{a_2,b_2}$, then $x' * 1 - \overline{x}' * a = k$, also. If $y' \neq y$ we have $x * a_1 \neq x' * a_1$ and this implies $x * 1 \neq x' * 1$. So, two different elements in $B_{a_1,b_1} \cap B_{a_2,b_2}$ produce two different occurrences of k in $[B_{1,0} - B_{a,0}]$. Conversely, if k occurs in $[B_{1,0} - B_{a,0}]$, we have $k = x'' * 1 - \overline{x}'' * a$ for $a = a_2 a_1^{-1}$, $k = (b_2 - b_1)a_1^{-1}$ and for some $x'', \overline{x}'' \in N$. Thus, there exists $y'' = x'' * a_1 + b_1 = \overline{x}'' * a_2 + b_2$ belonging to $B_{a_1,b_1} \cap B_{a_2,b_2}$. ♣

Now, to prove the following proposition, let O be a set of representatives of the Φ-orbits and remember that E is a set of representatives of the Φ-orbits covering C.

Proposition 2.5 *Let $\mathcal{D} = (N, \mathcal{B})$ be a wd-design. Let B_{a_1,b_1} and B_{a_2,b_2} be any two different blocks. Then*

$$max\{|B_{a_1,b_1} \cap B_{a_2,b_2}|, \ a_1, a_2 \in C, b_1, b_2 \in N\} = \\ = max\{f_{1,a,k}, \ (a,k) \in (E \times O) \setminus \{(1,0)\}\}$$

From Proposition 2.4 we know that $|B_{a_1,b_1} \cap B_{a_2,b_2}| = f_{1,a_2 a_1^{-1},(b_2-b_1)a_1^{-1}}$. When a_1, a_2 run over C, and b_1, b_2 run over N, $a_2 a_1^{-1}$ gives us all the elements of C and $(b_2 - b_1)a_1^{-1}$ gives us all the

elements of N. Moreover, we know that $N * a = N * \phi(a)$ and $f_{a_1,a_2,k} = f_{a_1,a_2,\phi(k)}$ for all $\phi \in \Phi$. So, to compute $max\{f_{1,a,k}, a \in C, k \in N\}$, we can confine a in E and k in O. Obviously, the case $(a = 1, k = 0)$ must be excluded because it would be to say that the two blocks coincide. ♣

Observation 2.6 Theorem 4.5 of [5] tells us something about the p_{ij}^k. Precisely, if two of U_i, U_j and U_k are contained in a proper subgroup N' of $(\mathbb{Z}_{p^n}, +)$ and the third one has an empty intersection with N', then $p_{ij}^k = p_{kj}^i = p_{ik}^j = 0$. To compute the non zero p_{ij}^k as well, we can also say that p_{ij}^k *equals the frequency of* d_k*, the representative of* U_k*, in the list* $[U_i - U_j]$ *of the differences between the element of* U_i *and those of* U_j*.*

3 Incidence matrix of a wd-design

If $\mathcal{B} = \{B_1, \ldots, B_b\}$ is a block design on $X = \{x_1, \ldots, x_v\}$ of parameters (v, b, r, k), the $v \times b$ matrix $A = (a_{yz})$ is called *incidence matrix* of the design when $a_{yz} = 1$ if $x_y \in B_z$ and $a_{yz} = 0$ if $x_y \notin B_z$.

Here we remember that a matrix of the form $\begin{pmatrix} c_0 & c_1 & \ldots & c_{n-1} \\ c_{n-1} & c_0 & \ldots & c_{n-2} \\ \vdots & \vdots & \ldots & \vdots \\ c_1 & c_2 & \ldots & c_0 \end{pmatrix}$ is called *circulant matrix* and, for a given circulant matrix C, we have

$$\det(C) = \prod_{j=1}^{n} f(\epsilon_j) \qquad \text{where} \qquad f(x) = \sum_{z=0}^{n-1} c_z x^z \tag{3.1}$$

is the defining polinomial of C and ϵ_1, ϵ_2, …, ϵ_n denote the distinct nth roots of unity, (see [9, 11]).

Now, we come back to the wd-designs previously constructed. We know that, for every choice of $\mathbb{Z}_{p^n}$ and $\Phi \subseteq Aut(\mathbb{Z}_{p^n}, +)$, our wd-designs are partially balanced with respect to the same association scheme with m associate classes, where either $m = f$, when $|\Phi|$ is even, or $m = f/2$, when $|\Phi|$ is odd, f being the number of the non trivial Φ-orbits.

For convenience, in what follows each element of $\mathbb{Z}_{p^n}$ will be denoted via his smallest non negative representative, that is $\mathbb{Z}_{p^n} = \{0, 1, \ldots, p^n - 1\}$.

Let $E = \{e_1, e_2, \ldots, e_c\}$ be a set of representatives of the Φ-orbits covering C. Consider the orbital wd-design $\mathcal{D}_{e_s} = (N, \mathcal{B}_{e_s})$ and set $B_{e_s,z} = N * e_s + z$, as usual. Let $A_s = (a_{yz})$ be the $p^n \times p^n$ incidence matrix of $\mathcal{D}_{e_s}$, where $a_{yz} = 1$ if, and only if, $y - 1 \in B_{e_s,z-1}$ and $a_{yz} = 0$ otherwise, for $y, z = 1, \ldots, p^n$. The incidence matrix of the union wd-design $\mathcal{D} = \left(N, \mathcal{B} = \bigcup_{e_s \in E} \mathcal{B}_{e_s}\right)$, is a $p^n \times cp^n$ matrix obtained by the juxtaposition of the A_ss, that is $A = (A_1 A_2 \ldots A_c)$.

Theorem 3.1 *Let* $\mathcal{D}_{e_s} = (N, \mathcal{B}_{e_s})$ *be an orbital wd-design with* m *associate classes and* A_s *its incidence matrix. Then, for* $s = 1, \ldots, c$

1. A_s *is a circulant matrix, symmetric if, and only if,* $|\Phi|$ *is even;*
2. $det(A_s) = k \prod_{j=1}^{p^n-1} \left(\sum_{z \in B_{1,0}} \epsilon^{jz} \right)$;
3. $H_s = A_s \cdot A_s^T$ *is a symmetric circulant matrix and* $det(H_s) = \prod_{j=1}^{p^n} \left(k + \sum_{i=1}^{m} (\lambda_i)_s \sum_{z \in U_i} \epsilon^{jz} \right)$

where ϵ *is a primitive* p^n*th root of unity and the* $(\lambda_i)_s$s *are the partial balance parameters of the* $\mathcal{D}_{e_s}$s*.*

1. A_s is circulant because $y-1 \in B_{e_s,z-1}$ if, and only if, $y \in B_{e_s,z}$, for $y,z = 1,\dots,p^n$. This implies $a_{yz} = a_{y+1\ z+1}$, subscripts *mod* p^n, for all $y,z = 1,\dots,p^n$. Now, let $|\Phi|$ be even. If $a_{y,1} = 1$, that is $y-1 \in B_{e_s,0}$, it results in $-(y-1) \in B_{e_s,0}$, because all the orbits are self paired. Hence $0 \in B_{e_s,y-1}$, that is $a_{1,y} = 1$. The converse is analogous, thus $a_{y,1} = a_{1,y}$ for $y = 1,\dots,p^n$. Using this last statement in addition to the circulant definition, when $y > z$ we have $a_{yz} = a_{y-(z-1),z-(z-1)} = a_{y-z+1,1} = a_{1,y-z+1} = a_{1+(z-1),y-z+1+(z-1)} = a_{zy}$, so we can conclude that A_s is symmetric.

2. Setting $a_{1,z} = c_{z-1}$ and applying (3.1), for $s = 1,\dots,c$ we have

$$det(A_s) = \prod_{j=1}^{p^n} \left(\sum_{z=0}^{p^n-1} c_z \epsilon_j^z \right) = \prod_{j=1}^{p^n} \left(\sum_{z=0}^{p^n-1} c_z \epsilon^{jz} \right) \tag{3.2}$$

where ϵ is a primitive p^nth root of unity and we set $\epsilon_j = \epsilon^j$. We know that $c_z = a_{1,z+1} = 1$ if, and only if, $0 \in B_{e_s,z}$ and this happens if, and only if, $-z \in B_{e_s,0}$, for $z = 0,\dots,p^n-1$.

If $|\Phi|$ is even, $-z \in B_{e_s,0}$ if, and only if, z itself belongs to $B_{e_s,0}$, because the Φ-orbits are self paired. So $c_z = 1 \iff z \in B_{e_s,0}$.

If $|\Phi|$ is odd, $-z \in B_{e_s,0}$ if, and only if, $z \in -B_{e_s,0} = \overline{B}_{e_s,0}$, the block containing all the orbits paired to the orbits of $B_{e_s,0}$. So $c_z = 1 \iff z \in \overline{B}_{e_s,0}$.

Thus, applying (3.2), for $s = 1,\dots,c$ we have

$$det(A_s) = \prod_{j=1}^{p^n} \left(\sum_{z \in B_{e_s,0}} \epsilon^{jz} \right) = \prod_{j=1}^{p^n} \left(\sum_{z \in jB_{e_s,0}} \epsilon^{z} \right) \quad \text{when } |\Phi| \text{ is even}$$

$$det(A_s) = \prod_{j=1}^{p^n} \left(\sum_{z \in \overline{B}_{e_s,0}} \epsilon^{jz} \right) = \prod_{j=1}^{p^n} \left(\sum_{z \in j\overline{B}_{e_s,0}} \epsilon^{z} \right) \quad \text{when } |\Phi| \text{ is odd}$$

where, obviously, $\overline{B}_{e_s,0} = B_{e_t,0}$, for some $t \in (1,\dots,c)$.

Finally, for every $s = 1,\dots,c$, we can see that $(B_{e_s,0}, 2B_{e_s,0}, \dots, p^n B_{e_s,0})$ becomes $\big(e_s(N*1), 2e_s(N*1), \dots, p^n e_s(N*1)\big)$, being $B_{e_s,0} = e_s(N*1)$. Since $\{e_s, 2e_s, \dots, p^n e_s\} = \mathbb{Z}_{p^n}$, rearranging the previous sequence we obtain $\big((N*1), 2(N*1), \dots, p^n(N*1)\big)$. Thus, $\forall s = 1,\dots,c$,

$$det(A_s) = \prod_{j=1}^{p^n} \left(\sum_{z \in B_{1,0}} \epsilon^{jz} \right) = k \prod_{j=1}^{p^n-1} \left(\sum_{z \in B_{1,0}} \epsilon^{jz} \right)$$

being $\sum_{z \in B_{1,0}} \epsilon^{p^n z} = |B_{1,0}| = k$.

3. The matrix $H_s = A_s \cdot A_s^T = (h_{yz})$ is obviously symmetric and circulant. The element h_{yz} give us the number of the blocks of $\mathcal{D}_{e_s}$ containing both the elements $y-1$ and $z-1$, hence $h_{yy} = k$, for $y = 1,\dots,p^n$. When $y \neq z$, $y-1$ and $z-1$ are i-associates if, and only if, their difference belongs to U_i. So, $z \in U_i$ implies $h_{1,z+1} = (\lambda_i)_s$, for $i = 1,\dots,m$. Applying again (3.1), where $c_z = h_{1,z+1}$, we can write

$$det(H_s) = \prod_{j=1}^{p^n} \left(\sum_{z=0}^{p^n-1} c_z \epsilon^{jz} \right) = \prod_{j=1}^{p^n} \left(k + \sum_{i=1}^{m} (\lambda_i)_s \sum_{z \in U_i} \epsilon^{jz} \right)$$

being $c_0 = k$ and $c_z = (\lambda_i)_s$ when $z \in U_i$, for $i = 1,\dots,m$. ♣

Theorem 3.2 *Let $\mathcal{D} = (N, \mathcal{B})$ be a union wd-design with m associate classes and $A = (A_1 A_2 \dots A_c)$ its incidence matrix. Then $H = A \cdot A^T$ is a symmetric circulant matrix and*

$$det(H) = \prod_{j=1}^{p^n} \left(r + \sum_{i=1}^{m} \lambda_i \sum_{z \in U_i} \epsilon^{jz} \right)$$

where the λ_is are the partial balance parameters of $\mathcal{D} = (N, \mathcal{B})$.

$H = A \cdot A^T$ is circulant because it is a sum of circulant matrices. The statement follows similarly to the point 3. of previous Theorem 3.1, but now $c_0 = \underbrace{k + \dots + k}_{c \ \ times} = ck = r$ and $c_z = \lambda_i = \sum_{s=1}^{c} (\lambda_i)_s$ when $z \in U_i$, for $i = 1, \dots, m$. ♣

4 Row and column codes from $PBIBD$s

A *binary code* of *length* n is a subset C of $\mathbb{Z}_2^n$. The *weight* of a codeword is the number of its non zero coordinate places. The *Hamming distance* between two codewords is the number of coordinate places in which they differ. The smallest of the distances between distinct codewords is called *minimum distance* of C and denoted by $d(C)$. A binary code of length n having m codewords and minimum distance d is called a *binary (n, m, d)-code*. If C is a vector subspace of $\mathbb{Z}_2^n$ and $dim(C) = k$, then it is called a binary *linear (n, k)-code*.

It is well known that there is a link between block designs and codes via the design incidence matrix A: the set of all the columns, the set of all the rows of A, as well as their linear hulls can be regarded as binary codes and A itself can be regarded as the parity check matrix of a linear code. For more information on codes see [1, 12].

In what follows we are interested in the set C_c of all the columns of A and the set C_r of all the rows of A, the so called *column code* and *row code*, respectively. The parameters characterizing C_c and C_r depend on the design parameters, as we summarize in the following proposition.

Proposition 4.1 *Let $\mathcal{B}$ be a $PBIBD$ with parameters $(v, b, r, k, \lambda_1, \dots, \lambda_m)$, A its incidence matrix, $\mathcal{C}_r$ and $\mathcal{C}_c$ the related row and column codes. Set $\lambda = max\{\lambda_1, \dots, \lambda_m\}$ and $\mu = max\{|B_i \cap B_j|, i, j = 1, \dots, b \quad with \quad i \neq j\}$. Then*

(1) the cardinality of $\mathcal{C}_r$ is v, the codeword length is b, each codeword has the same weight r and the minimum distance is $d(\mathcal{C}_r) = 2(r - \lambda)$.

(2) the cardinality of $\mathcal{C}_c$ is b, the codewords length is v, each codeword has the same weight k and the minimum distance is $d(\mathcal{C}_c) = 2(k - \mu)$. ♣

4.1 Row and column codes from wd-designs

Now, we come back to the $PBIBD$s of [5], the so called *wd-designs* recalled in Paragraph 2, and we consider their incidence matrices. Working on $\mathbb{Z}_{p^n}$ with $|\Phi| = tp^h$, each orbital design has a $p^n \times p^n$ matrix A_i, for $i = 1, \dots, c$, and $A = (A_1 \dots A_c)$ is the incidence matrix of the union block design. We can see that, applying previous Propositions and using the keys of Paragraph 2.1.2, we are able to compute all the wd-design parameters as well as those of the row and column codes related to their incidence matrices and we obtain:

row and column codes					
design	code	words	length	d	weight
$\mathcal{D}_a = (N, \mathcal{B}_a)$	C_r or C_c	p^n	p^n	$2(k-\lambda_a)$	k
$\mathcal{D} = (N, \mathcal{B})$	C_r	p^n	cp^n	$2(ck-\lambda)$	ck
	C_c	cp^n	p^n	$2(k-\mu)$	k

where $k = \dfrac{p^{h+1}-1}{p-1}t + (n-h-1)t + 1$, $c = \dfrac{p-1}{t}p^{n-h-1}$, $\lambda_a = max\left\{f_{1,d_i a^{-1}},\ d_i \in D\right\}$,

$$\lambda = max\left\{\sum_{e_j \in E} f_{1,d_i e_j},\quad d_i \in D\right\},\ \mu = max\left\{f_{1,a,k},\ (a,k) \in (E \times O) \setminus \{(1,0)\}\right\}.$$

5 Some special classes of wd-designs

From the key of page 4 we know that the number m of the associate classes of a wd-design is f or $f/2$, according to the order of Φ is even or odd.

Thus, if we want a given number of associate classes, we have to compute case by case. For example, if we want an eight-class wd-design, we can work on $\mathbb{Z}_{3^8}$ with $|\Phi| = 3^7$ as well as on $\mathbb{Z}_{5^4}$ with $|\Phi| = 2.5^3$ as well as on $\mathbb{Z}_{13^4}$ with $|\Phi| = 3.13^3$ and so on.

Now, two special cases will be examined, for which the previous formulae can be developed further.

5.1 The case with $|\Phi| = p^{n-1}$

We are following the line described in Section 2, Paragraph 2.1.

First step. In $Aut(\mathbb{Z}_{p^n})$ we choose $\Phi =< \alpha_{p+1} >$ [2], thus $|\Phi| = p^{n-1}$. So we start from $p = p$, $n = n$, $h = n-1$ and $t = 1$. Using the keys of Paragraph 2.1.2 we can compute the number c of the Φ-orbits covering $C = \mathbb{Z}_{p^n} \setminus p\mathbb{Z}_{p^n}$: $c = p-1$. Now we have to select a set E of representatives of these Φ-orbits and, for convenience, we want $1 \in E$. An easy selection is $E = (e_j)_{j \in I_{p-1}} = (1, 2, \ldots, p-1)$. Now, from [4], we learn that a new multiplication "$*$" can be defined on $\mathbb{Z}_{p^n}$ to obtain a wd-nearring $N = (\mathbb{Z}_{p^n}, +, *)$ and we have $N * 1 = \Phi(1) \cup \Phi(p) \cup \cdots \cup \Phi(p^{n-1}) \cup \{0\}$ (see Paragraph 2.1.1), where $\Phi(p^s) = \{p^s + h_{s+1}p^{s+1},\ \ 0 \le h_{s+1} < p^{n-s-1}\}$, for $s = 0, \ldots, n-1$.

Second step. Using the sets $N * a + b$, with $a \in C$ and $b \in N$, as blocks, wd-designs can be constructed. We have $p-1$ *orbital wd-designs*, generated by the $p-1$ basic blocks $N*1, \ldots, N*(p-1)$ and isomorphic to each other, of parameters $v = b = p^n$ and $k = r = (p^n + p - 2)/(p-1)$ and one *union wd-design*, union of the previous ones, of parameters $v = p^n$, $b = (p-1)p^n$, $k = (p^n + p - 2)/(p-1)$ and $r = p^n + p - 2$.

Third step. Using the keys of Paragraph 2.1.2 we can compute the number of the non trivial Φ-orbits, $f = n(p-1)$. As $|\Phi|$ is odd, we know that the non trivial Φ-orbits are not self-paired, so we define the U_is by pairing them, that is $U_i = \Delta_i \cup -\Delta_i$, with $i = 1, \ldots, f/2$. Thus, we obtain an association scheme with $m = n(p-1)/2$ associate classes defining x and y to be ith associates when $x - y$ belongs to U_i. To compute the association scheme parameters, the U_is have to be ordered and we can do it by choosing D, a set of their representatives: $D = (d_i)_{i \in I_m} = \left(1, 2, \ldots, \frac{p-1}{2}, p, 2p, \ldots, \frac{p-1}{2}p, \ldots, p^{n-1}, 2p^{n-1} \ldots, \frac{p-1}{2}p^{n-1}\right)$. We know that the number of the ith

[1] for $s \in \mathbb{Z}$ and $(s,p) = 1$, α_s is the automorphism of $\mathbb{Z}_{p^n}$ s. t. $\alpha_s(x) = sx, \forall x \in \mathbb{Z}_{p^n}$.

associates of each element depends on i only, and now we have $n_i = |U_i|$, thus $n_i = 2p^{n-j}$, where $j = 1, \ldots, n$ and $i = (j-1)(p-1)/2 + 1, \ldots, j(p-1)/2$.
Since $m = n(p-1)/2$, the p_{ij}^k fill in $n(p-1)/2$ squared matrices of order $n(p-1)/2$: the P_ks. Now, applying the first part of Observation 2.6, we obtain the general structure of these matrices. In fact, for $l = 1, \ldots, n$, if one of k, i or j belongs to $\{(l-1)(p-1)/2+1, \ldots, l(p-1)/2\}$ and the two others are greater than $l(p-1)/2$, we have $p_{ij}^k = p_{kj}^i = p_{ik}^j = 0$. So, setting

$$Q_{k\ r} = (p_{ij}^k) \quad \text{with} \quad i,j = (r-1)\tfrac{p-1}{2}+1, \ldots, r\tfrac{p-1}{2}, \quad r = 1, \ldots, n$$

$$H_{k\ r+s} = (p_{ij}^k) \quad \text{with} \begin{cases} i = (r-1)\frac{p-1}{2}+1, \ldots, r\frac{p-1}{2}, & r = 1, \ldots, n \\ j = (r+s-1)\frac{p-1}{2}+1, \ldots, (r+s)\frac{p-1}{2} & s = 1, \ldots, n-r \end{cases}$$

for $l = 1, \ldots, n$ and $k = (l-1)(p-1)/2+1, \ldots, l(p-1)/2$, we obtain

$$P_k = \left(\begin{array}{ccc|ccc} Q_{k\ 1} & \ldots & 0 & & & \\ \vdots & \vdots & \vdots & & \underline{0} & \\ 0 & \ldots & Q_{k\ l-1} & & & \\ \hline & & & Q_{k\ l} & H_{k\ l+1} \ldots & H_{k\ n} \\ & \underline{0} & & H_{k\ l+1}^T & 0 \ldots & 0 \\ & & & \vdots & \vdots & \vdots \\ & & & H_{k\ n}^T & 0 \ldots & 0 \end{array}\right)$$

Fourth step. To compute the partial balance parameters applying the keys of Paragraph 2.1.2, we need the frequencies f_{1,d_ie_j} for $d_i \in D$ and $e_j \in E$. Actually, it is sufficient to compute $f_{1,1} = 1+1+p+\cdots+p^{n-2} = 1+\frac{p^{n-1}-1}{p-1}$, $f_{1,2} = \cdots = f_{1,(p-1)/2} = 0$, and, for $h = 1, \ldots, n-1$, $f_{1,p^h} = p^{n-1}+p^{n-2}+\cdots+p^{n-h}+1+\frac{p^{n-h-1}-1}{p-1}$, $f_{1,2p^h} = \cdots = f_{1,p^h(p-1)/2} = p^{n-1}+p^{n-2}+\cdots+p^{n-h}$, to obtain

for $\mathcal{D}_1$, the *orbital wd-design* generated by $B_{1,0} = N * 1$ with $(\lambda_i)_1 = f_{1,d_i \cdot 1} = f_{1,d_i}$
for $h = 0, \ldots, n-1$
$\lambda_{h(p-1)/2+1} = f_{1,p^h} = p^{n-1}+p^{n-2}+\cdots+p^{n-h}+1+\frac{p^{n-h-1}-1}{p-1}$
$\lambda_{h(p-1)/2+2} = f_{1,2p^h} = \cdots = \lambda_{(h+1)(p-1)/2} = f_{1,p^h(p-1)/2} = p^{n-1}+p^{n-2}+\cdots+p^{n-h}$
$\lambda = max\{\lambda_1, \ldots, \lambda_{n(p-1)/2}\} = \frac{p^n-1}{p-1}$

For $\mathcal{D}_2, \ldots, \mathcal{D}_{p-1}$ we find the same values but, obviously, not in the same order.

for $\mathcal{D}$, the *union wd-design*
for $h = 0, \ldots, n-1$
$\lambda_{h(p-1)/2+1} = \sum_{e_j \in E} f_{1,d_{h(p-1)/2+1}e_j} = 2(f_{1,p^h} + f_{1,2p^h} + \cdots + f_{1,p^h(p-1)/2}) =$
$2 + p^n - p^{n-h} + 2\frac{p^{n-h-1}-1}{p-1} = \lambda_{h(p-1)/2+2} = \cdots = \lambda_{(h+1)(p-1)/2}$
$\lambda = max\{\lambda_1, \ldots, \lambda_{n(p-1)/2}\} = p^n - p + 2$

There remains to compute μ, the maximum cardinality of the block intersections. Obviously, for each orbital wd-design we have $\mu = \lambda$. For the union wd-design, applying Proposition 2.5, we have to compute the $f_{1,a,k}$s, for $(a,k) \in (E \times O) \setminus \{(1,0)\}$. E was already defined as $(1, 2, \ldots, p-1)$. O, a set of representatives of all the Φ-orbits, can be taken as $O = E \cup pE \cup \cdots \cup p^{n-1}E \cup \{0\}$. After a straightforward computation we obtain again $\mu = (p^n-1)/(p-1)$. Thus, applying the key of Paragraph 4.1, for the row and column codes we have:

row and column codes					
wd-design	code	words	length	d	weight
$\mathcal{D}_1,\dots,\mathcal{D}_{p-1}$	C_r or C_c	p^n	p^n	2	$(p^n+p-2)/(p-1)$
$\mathcal{D}$	C_r	p^n	$(p-1)p^n$	$4(p-2)$	(p^n+p-2)
	C_c	$(p-1)p^n$	p^n	2	$(p^n+p-2)/(p-1)$

Finally, applying Theorems 3.1 and 3.2, for the incidence matrix we obtain:

incidence matrix $A=(A_1\dots A_{p-1})$
$\displaystyle\lvert A_1\rvert=\dots=\lvert A_{p-1}\rvert=k\prod_{j=1}^{n-1}\left[\frac{p^{jp}+(p^{j-1}+\dots+p+2)^p}{p^j+\dots+p+2}\right]^{p^{n-j-1}}$
$\lvert A\cdot\ A^T\rvert=$ $\displaystyle(p-1)k^2\prod_{h=0}^{n-1}\left[(p-1)k-p^h\lambda_{(n-h)\frac{p-1}{2}}+(p-1)\sum_{a=0}^{h-1}p^a\lambda_{(n-a)\frac{p-1}{2}}\right]^{p^{n-h-1}(p-1)}$

5.2 The case with $|\Phi|=\frac{p-1}{2}p^{n-1}$

Following, as above, the line of Paragraph 2.1.1 of Section 2, if we work on $\mathbb{Z}_{p^n}$ and we choose $|\Phi|=\frac{p-1}{2}p^{n-1}$ with $p\equiv 3(mod 4)$, we obtain an already known class of $PBIBD$s. The union wd-design $\mathcal{D}=(N,\mathcal{B})$ can be split into two orbital wd-designs $\mathcal{D}_1=(N,\mathcal{B}_1)$, generated by $B_{1,0}=N*1$, and $\mathcal{D}_2=(N,\mathcal{B}_2)$ generated by $B_{p^n-1,0}=N*(p^n-1)$. All the designs have the same association scheme with n associate classes and they, their incidence matrices and the related row and column codes are described in the following tables:

association scheme		
$x,y\in\mathcal{R}_i$	ith associate elements, for $i=1,\dots,n$	if $x-y\in U_i=p^{i-1}\mathbb{Z}_{p^n}\setminus p^i\mathbb{Z}_{p^n}$
m	number of the associate classes	$m=f/2=n$
n_i	number of the ith associates elements	$n_i=(p-1)p^{n-i}$ for $i=1,\dots,m$

As usual we set $P_k=(p_{ij}^k)$ for $k=1,\dots,m$

$$P_k=\begin{pmatrix} n_1 & 0 & \dots & 0 & 0 & 0 & \dots & 0\\ 0 & n_2 & \dots & 0 & 0 & 0 & \dots & 0\\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & \dots & n_{k-1} & 0 & 0 & \dots & 0\\ 0 & 0 & \dots & 0 & (p-2)p^{n-k} & n_{k+1} & \dots & n_m\\ 0 & 0 & \dots & 0 & n_{k+1} & 0 & \dots & 0\\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & \dots & 0 & n_m & 0 & \dots & 0 \end{pmatrix}$$

	tactical configuration				partial balance
design	v	b	k	r	λ_i for $i=1,\dots,n$
$\mathcal{D}_1$ or $\mathcal{D}_2$	p^n	p^n	$\frac{p^n+1}{2}$	$\frac{p^n+1}{2}$	$(\lambda_i)_1=(\lambda_i)_2=(2p^n-p^{n-i+1}-p^{n-i}+2)/4$
$\mathcal{D}$	p^n	cp^n	$\frac{p^n+1}{2}$	p^n+1	$\lambda_i=(2p^n-p^{n-i+1}-p^{n-i}+2)/2$

incidence matrix $A = (A_1 A_2)$		
$A_1 = A_2^T \qquad A_1 + A_2 = J + I \qquad A * A^T = 2(A_1 * A_1^T) = 2(A_2^T * A_2)$		
A_s	incidence matrix of $\mathcal{D}_s = (N, \mathcal{B}_s) \quad s = 1, 2$	$\lvert A_1\rvert = \lvert A_2\rvert = k \prod_{j=1}^{n} \left[\left(1 + p^{2(n-j)+1}\right)/4\right]^{p^{j-1}(p-1)/2}$
A	incidence matrix of $\mathcal{D} = (N, \mathcal{B})$	$\lvert A \cdot {}^t A\rvert = 2k^2 \prod_{j=1}^{n} \left[\left(1 + p^{2(n-j)+1}\right)/2\right]^{p^{j-1}(p-1)}$

row and column codes					
design	code	words	length	d	weight
$\mathcal{D}_1$ or $\mathcal{D}_2$	C_r or C_c	p^n	p^n	$(p+1)/2$	$(p^n+1)/2$
$\mathcal{D}$	C_r	p^n	$2p^n$	$p+1$	p^n+1
	C_c	$2p^n$	p^n	$(p+1)/2$	$(p^n+1)/2$

References

[1] Assmus Jr., E.F. and Key, J.D., *Designs and their codes*, Cambridge Tractas in Mathhematics, Cambridge University Press, NY 1992.

[2] Bannai, E., *Introduction to association schemes*, Methods of Discrete Mathematics, (Braunschweig,1999), 1-70.

[3] Benini, A. and Morini, F., *Weakly divisible nearrings on the group of integers (mod p^n)*, Riv. Mat. Univ. Parma, (6) **1** (1998), 1-11.

[4] Benini, A. and Morini, F., *On the construction of a class of weakly divisible nearrings*, Riv. Mat. Univ. Parma, (6) **1** (1998), 103-111.

[5] Benini, A. and Morini, F., *Partially Balanced Incomplete Block Designs from Weakly Divisible Nearrings*, Sem. Mat. Brescia, Quad. 17 (2004), preprint.

[6] Benini, A. and Pellegrini, S., *Weakly Divisible Nearrings*, Discrete Math. 208/209 (1999), 49-59.

[7] Beth, T., Jungnickel, D. and Lenz, H., *Design Theory*, Encyclopedia of Mathematics and its Applications, 69. Cambridge University Press, Cambridge 1999.

[8] Clay, J.R., *Nearrings: Geneses and Applications*, Oxford Science Publications, Oxford University Press, NY 1992.

[9] Davis, P.J., *Circulant matrices*, 2nd. ed., Chelsea Publishing, New York, NY 1994.

[10] Hall, M., *Designs with transitive authomorphism group*, Proc. of Symposia in Pure Math. AMS, T. L. Motzkin, ed., (1971), 109-113.

[11] Lancaster, P. and Timenetsky, M., *The theory of matrices*, 2nd. ed. ACADEMIC PRESS, 1985.

[12] McWilliams, F.J. and Sloane, N.J.A., *The theory of Error-correcting Codes*, North-Holland Amsterdam 1977.

[13] Penfold Street, A. and Street, D.J., *Combinatorics of Experimental Design* Oxford University Press, New York, 1987.

[14] Pilz, G., *Near-rings*, 2nd. ed., North Holland Math. Studies 23, Amsterdam, 1983.

Anna Benini,
Dipartimento di Matematica,
Facoltà di Ingegneria,
Università degli Studi di Brescia,
Via Valotti 9, I-25133 BRESCIA, Italy.
Email: anna.benini@ing.unibs.it

Eingegangen am 13. Dezember 2004