Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 301 (2005) 34–45

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Partially balanced incomplete block designs from weakly divisible nearrings☆

A. Benini*, F. Morini

Dipartimento di Matematica, Facoltà di Ingegneria, Università degli Studi di Brescia, Via Valotti 9, I-25133 Brescia, Italy

Received 31 July 2002; received in revised form 21 September 2004; accepted 7 March 2005
Available online 18 August 2005

Abstract

In [[6] Riv. Mat. Univ. Parma 11 (2) (1970) 79–96] Ferrero demonstrates a connection between a restricted class of planar nearrings and balanced incomplete block designs. In this paper, bearing in mind the links between planar nearrings and weakly divisible nearrings (wd-nearrings), first we show the construction of a family of partially balanced incomplete block designs from a special class of wd-nearrings; consequently, we are able to give some formulas for calculating the design parameters.

Keywords: Block design; Association scheme; Nearring

1. Introduction

A nearring N is called a *weakly divisible nearring* (wd-nearring) if the following condition is satisfied: $\forall a, b \in N\ \exists x \in N | ax = b$ or $bx = a$. This algebraic structure was first defined and studied in [4] and a method to construct a special class of wd-nearrings was found in [2,3]. This method has been generalized and implemented in " SONATA", a package of GAP [1].

The structure of a finite wd-nearring is quite similar to that of a better known planar nearring. Since planar nearrings have been a powerful tool in the construction of balanced

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

* Corresponding author.
E-mail address: anna.benini@ing.unibs.it (A. Benini).

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.03.026

incomplete block designs (BIB-designs), in this paper it is shown that partially balanced incomplete block designs (PBIB-designs) can be constructed from a class of wd-nearrings. More precisely, the paper is organized as follows:

In Section 2 we gather some results on wd-nearrings which we will use throughout the paper.

In Section 3, using the structure and the properties of a suitable class of wd-nearrings, we show how it is possible to construct block designs and to compute their parameters.

In Section 4 we firstly recall that, starting from an orbital design and using a general construction of Hall, it is possible to define an association scheme making the design a PBIB-design. Then, we prove that the previously constructed designs are orbital designs or a disjoint union of them. Thus, such designs become partially balanced and several formulas to compute their parameters are proved.

In Section 5, to facilitate the application of the many steps of the whole construction, we will conclude showing an example.

2. Weakly divisible 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 [5,9]). In the sequel we always consider left *zerosymmetric* nearrings, that is, $0 * x = 0, \ \forall x \in N$.

In this section, we shall summarize the results, terminology and notation from [4,2,3] that will be used in the sequel.

Definition 2.1. A nearring N is called weakly divisible (wd-nearring) if the following condition is satisfied:

$$\forall a, b \in N \ \exists x \in N \mid ax = b \text{ or } bx = a.$$

In [4] it is proved that a finite wd-nearring N is the disjoint union of the nil radical Q (the set of the nilpotent elements of N) and the multiplicative semigroup C of the left cancellable elements. Moreover, by Theorem 8 of [4], the set C is the disjoint union of its maximal multiplicative subgroups, isomorphic to each other. As in [2], γ_a denotes the left translation defined by a, for $a \in N$, that is, $\gamma_a(x) = ax$, for every $x \in N$. We know that γ_a is an endomorphism of N^+ which turns out to be an automorphism if, and only if, a is a left cancellable element of N. Furthermore, by Proposition 2 of [2] we note that $\Gamma(C)$, the set of the left translations defined by the elements of C, is an automorphism group of N^+ with respect to composition, and the fixed points of $\gamma_c \neq id_N$, $c \in C$, are nilpotent elements of N.

Definition 2.2. Let p be a prime number and consider the residue class group (*modulo* p^n) $(\mathbb{Z}_{p^n}, +)$. A p^n-maximal wd-nearring N is a finite wd-nearring on $(\mathbb{Z}_{p^n}, +)$, in which the set Q of the nilpotent elements of N coincides with $p\mathbb{Z}_{p^n}$.

Obviously, the ring $\mathbb{Z}_{p^n}$ is, in particular, a p^n-maximal wd-nearring but this trivial case will be excluded in the following.

In [2,3] p^n-maximal wd-nearrings are investigated and a construction method is shown. In this paper we will limit our attention to the case where p is odd. Theorem 2.5 summarizes the results from Theorems 2,3 of [2] and Theorem 1 of [3], needed in the sequel.

Definition 2.3. Let G be a group. Let $H \leqslant G$ and $\Phi \leqslant Aut(G)$. For each orbit $\Phi(g)$, $g \in G$, the set of the cosets of H which contain elements of $\Phi(g)$ is called H-class of $\Phi(g)$, denoted by $[\Phi(g)]_H$.

Definition 2.4. Let G be a group. Let $H \leqslant G$ and $\Phi \leqslant Aut(G)$. Two orbits $\Phi(g)$ and $\Phi(g')$, $g, g' \in G$, are called H-equivalent if $[\Phi(g)]_H = [\Phi(g')]_H$.

To simplify our notations, when H is cyclic we identify H with its generator h and, so, we briefly say h-class (or h-equivalent) and write $[\Phi(g)]_h$.

Theorem 2.5. *Let p be an odd prime number. Let $G = (\mathbb{Z}_{p^n}, +)$ and $\Phi \leqslant Aut(G)$. Suppose E is a set of the representatives of the orbits of Φ included in $\mathbb{Z}_{p^n} \setminus p\mathbb{Z}_{p^n}$ such that the selected representatives of p-equivalent orbits belong to the same coset of $p\mathbb{Z}_{p^n}$. Choose e in E. Define*[1]:

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

Then $N = (\mathbb{Z}_{p^n}, +, *)$ is a p^n-maximal wd-nearring.

Conversely, every p^n-maximal wd-nearring $N = (\mathbb{Z}_{p^n}, +, \circ)$ coincides with the one constructed as below, starting from the group $G = (\mathbb{Z}_{p^n}, +)$ and choosing $\Phi = \Gamma(C)$, E as the set of the idempotent elements of N and e coinciding with an idempotent right identity of the residue class p.

3. Block designs from wd-nearrings

The object of this section is to prove Theorem 3.8, in which we state that a class of cyclic block designs is constructible starting from a wd-nearring N, obtained as in Theorem 2.5.

In the following, most of the notation and terminology for design theory is that used by [8]. Here we recall that an incidence structure $(X, \mathscr{B} \subseteq \mathscr{P}(X))$ on a finite set X is called *block design* (or *tactical configuration*) if all the blocks contain the same number k of elements and all the elements 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, and *cyclic* if it has a cyclic automorphism group regular on X.

The numbers (v, b, r, k), where v and b are the cardinality of X and $\mathscr{B}$ respectively, are called the *parameters* of the design. It is well known that they are not independent, because $vr = bk$.

[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 $\Phi(x)$.

Definition 3.1. Let N be a p^n-maximal wd-nearring. The set $N * a + b$, a, b fixed in N, is called the block determined by a, b and denoted by $B_{a,b}$. A block of the form $N * a$ is called a basic block generated by a.

Proposition 3.2. *Let N be a p^n-maximal wd-nearring. If $\Phi = \Gamma(C)$ has order tp^h, $(t, p) = 1$, then there are $c = \frac{p-1}{t} p^{n-h-1}$ distinct basic blocks generated by the elements of C.*

First we will show that if a, b belong to C then $N * a = N * b$ if, and only if, a and b belong to the same Φ-orbit. From [4] we learn that $a \in C$ implies $a \in N * a$. Hence $N * a = N * b$ implies $a \in N * b$, that is, $a = y * b$ for some $y \in N$. So y cannot be nilpotent; otherwise, $y * b = a$ ought to be nilpotent. Thus y is a cancellable element and, applying Theorem 2.5, we have $a = y * b = b\phi_y(1) = \phi_y(b)$. The converse is analogous.

We conclude that the number c of the distinct basic blocks equals the number $\frac{|C|}{|\Phi|}$ of the Φ-orbits covering C, that is, $c = \frac{p-1}{t} p^{n-h-1}$.

Remark 1. The cardinality of a basic block depends on its generator. Generally, if a is a cancellable element and q is a nilpotent, the cardinality of $N * a$ is greater than that of $N * q$. That is why, in order to obtain a tactical configuration, only basic blocks generated by cancellable elements will be considered. Moreover, since our claim is to obtain an incomplete block design, we must exclude the case $N = N * a + b$, for all $a, b \in N$. Thus we will not consider the trivial case $\Gamma(C) = Aut(N^+)$, in which the wd-nearring is a ring.

Hereinafter p^n-maximal wd-nearring means *p is an odd prime number* and *the nearring is not a ring*.

Proposition 3.3. *Let Φ be a subgroup of $Aut(\mathbb{Z}_{p^n}, +)$ of order tp^h, $(t, p) = 1$. Then*

$$|\Phi(p^r)| = \begin{cases} t, & r \geqslant h, \\ tp^{h-r}, & r \leqslant h. \end{cases}$$

Denote $G = (\mathbb{Z}_{p^n}, +)$. It is well-known that $\Phi = T \times \Phi_h$, where $T \leqslant Aut(G)$ is a group of order t of fixed point free automorphisms of G and $\Phi_h = \{\gamma_k : a \to ka \mid k = bp^{n-h} + 1,\ 0 \leqslant b \leqslant p^h - 1\} \leqslant Aut(G)$ has order p^h (see [5, Chapter 2, p. 49]). If $r \geqslant h$, p^r is fixed by each automorphism of Φ_h, so $|\Phi(p^r)| = t$. Let $r < h$. The automorphisms of Φ_h fixing p^r are of the form γ_k, where $k = bp^{n-h} + 1$ with $b \equiv 0 \pmod{p^{h-r}}$. The b elements satisfying all our conditions are exactly p^r, thus $|\Phi(p^r)| = \frac{|\Phi|}{p^r} = tp^{h-r}$.

Proposition 3.4. *Let N be a p^n-maximal wd-nearring and $a \in C$. If $\Phi = \Gamma(C)$ has order tp^h, $(t, p) = 1$, then $N * a = \bigcup_{r=1}^{n-1} \Phi(ap^r e^{-r}) \cup \{0\} \cup \Phi(a)$ and $|N * a| = \frac{p^{h+1}-1}{p-1} t + (n-h-1)t + 1$.*

Obviously, $(a, p) = 1$ and $N * a = a(N * 1)$ imply $|N * a| = |N * 1|$, for all $a \in C$. If $x = kp^r$, with $k \in \mathbb{Z}$ and $(k, p) = 1$, from Theorem 2.5 we learn that $x * 1 = p^r \phi_{ke^r}(e^{-r})$, so $N * 1 = Q * 1 \cup C * 1 = \bigcup_{r=1}^{n-1} \{kp^r * 1 | k \in \mathbb{Z}, (k, p) = 1\} \cup \{0\} \cup \Phi(1)$ (see [4, Proposition 9]). From Proposition 5 of [2] we know that $kp^r * 1 = ke^r * e^{-r} p^r$, for all

$r = 1, \ldots, n-1$, moreover, it is clear that the set $\{k\mathrm{e}^r \mid k \in \mathbb{Z}, (k, p) = 1\}$ equals C, so $\{kp^r * 1 \mid k \in \mathbb{Z}, (k, p) = 1\} = \{k\mathrm{e}^r * \mathrm{e}^{-r}p^r \mid k \in \mathbb{Z}, (k, p) = 1\} = \Phi(\mathrm{e}^{-r}p^r)$. Thus $N * 1 = \bigcup_{r=1}^{n-1} \Phi(\mathrm{e}^{-r}p^r) \cup \{0\} \cup \Phi(1)$. Since $|\Phi(\mathrm{e}^{-r}p^r)| = |\Phi(p^r)|$, the previous statement gives us $|N*1| = \sum_{r=1}^{h} |\Phi(p^r)| + \sum_{r=h+1}^{n-1} |\Phi(p^r)| + 1 + |\Phi| = \sum_{r=0}^{h} |\Phi(p^r)| + \sum_{r=h+1}^{n-1} |\Phi(p^r)| + 1$. By Proposition 3.3 we obtain $|N * 1| = \sum_{r=0}^{h} tp^{h-r} + t(n-h-1) + 1 = t(p^{h+1} - 1)(p-1)^{-1} + t(n-h-1) + 1$.

Proposition 3.5. *Let N be a p^n-maximal wd-nearring. Then $N * 1 + b = N * 1$ if, and only if, $b = 0$.*

If $b = 0$ the statement is trivial. Suppose $N * 1 + b = N * 1$, $b \neq 0$. Obviously b belongs to $N * 1$, as $0 + b = b$. Thus $N * 1$ contains the cyclic additive subgroup $\langle b \rangle$, generated by b. This implies $b \in Q$, otherwise, $N = N * 1$ and this is excluded since N is not a ring. So, set $b = kp^r$, where $k \in \mathbb{Z}$ and $(k, p) = 1$. From $\langle b \rangle \subseteq N * 1$ we know that $\langle b \rangle = \bigcup_{i=r}^{n-1} \Phi(\mathrm{e}^{-i}p^i) \cup \{0\}$. Hence the orbit of $\mathrm{e}^{-r}p^r$ contains all the elements of Q which are multiples of p^r but not of p^{r+1}, which means $|\Phi(\mathrm{e}^{-r}p^r)| = (p-1)p^{n-(r+1)}$. If $r < h$, from Proposition 3.3 we know that $|\Phi(\mathrm{e}^{-r}p^r)| = tp^{h-r}$, so $h = n-1$, $t = p-1$ and we obtain $\Phi = Aut(N^+)$, which implies $N = N * 1$, now excluded as N is not a ring. If $r \geqslant h$, again from Proposition 3.3, we have $|\Phi(\mathrm{e}^{-r}p^r)| = t$, so $r = n-1$ and $t = p-1$, hence, $b = kp^{(n-1)}$. Thus, $\langle b \rangle = \{0\} \cup \Phi(\mathrm{e}^{-(n-1)}p^{n-1})$ and this implies $\{0\} \cup \Phi(\mathrm{e}^{-(n-1)}p^{n-1}) = (\{0\} \cup \Phi(\mathrm{e}^{-(n-1)}p^{n-1})) + b$. The last equality forces $\Phi(\mathrm{e}^{-i}p^i) = \Phi(\mathrm{e}^{-i}p^i) + b$, $i = 1, \ldots, n-2$. In particular, now we consider $i = h$. We know that $|\Phi(\mathrm{e}^{-h}p^h)| = t = p-1$; hence, $\mathrm{e}^{-h}p^h + b = \alpha(\mathrm{e}^{-h}p^h)$, where α is a fixed point free automorphism of N. Thus, $\mathrm{e}^{-h}p^{h+1} + pb = \alpha(\mathrm{e}^{-h}p^{h+1})$ and the element $\mathrm{e}^{-h}p^{h+1}$ is a fixed point of α, as $pb = 0$. This implies that $h = n-1$ and again $\Phi = Aut(N^+)$, which is excluded.

Proposition 3.6. *Let N be a p^n-maximal wd-nearring. Then $B_{a,b} = B_{c,d}$ if, and only if, $N * a = N * c$ and $b = d$.*

Obviously, $N * a = N * c$ and $b = d$ imply $B_{a,b} = B_{c,d}$. Suppose $B_{a,b} = B_{c,d}$ and $d - b \neq 0$. From $N * a = N * c + (d-b)$ we obtain $N * 1 = N * a^{-1}c + (d-b)a^{-1}$. Set $g = a^{-1}c$ and $f = (d-b)a^{-1}$ to obtain $N * 1 = N * g + f$. From previous equality $u * N * 1 = u * N * g + u * f$, for all $u \in C$, and also $N * 1 = N * g + u * f$, since $u * N = N$. So $N * 1 = N * 1 + u * f - f$ and Proposition 3.5 forces $u * f = f$, for all $u \in C$. This means f is a fixed point for all the elements of Φ, so $\Phi = \Phi_h$ and $f = kp^r$, where $r \geqslant h$ and $(k, p) = 1$. For all $m \in \mathbb{Z}$, $(m, p) = 1$, and for all $i \geqslant h$, $\Phi = \Phi_h$ implies $\Phi(mp^i) = \{mp^i\}$; hence, for all $u \in C$, $u * mp^i = mp^i$, and thus $mp^i * 1 = m\mathrm{e}^i * \mathrm{e}^{-i}p^i = \mathrm{e}^{-i}p^i$. This implies that, for all $i \geqslant h$, $g\mathrm{e}^{-i}p^i$ and $\mathrm{e}^{-i}p^i$ are the only multiples of p^i, but not of p^{i+1}, belonging to $N * g$ and $N * 1$, respectively. Hence $mp^{n-1} * g + f = \mathrm{e}^{-r}p^r$, as $h \leqslant n-1$. From $h < n-1$, we also obtain $mp^{n-2} * g + f = \mathrm{e}^{-r}p^r$, the only multiple of p^r, but not of p^{r+1}, belonging to $N * 1$, and this is impossible because $mp^{n-1} * g \neq mp^{n-2} * g$. Hence it must be $h = n-1$, which implies $r = n-1$, as $h \leqslant r$. So, from $g + f \in \Phi(1)$, we have $g + kp^{n-1} = 1 + hp^{n-1}$, for some $h \in \mathbb{Z}$, hence, $g \in \Phi(1)$ and this forces $\Phi(g) = \Phi(1)$. In this way we end up with $N * g = N * 1$, which is excluded.

Lemma 3.7. *Let N be a p^n-maximal wd-nearring with $|\Gamma(C)| = tp^h$, $(t, p) = 1$. Fix $a \in C$ and set $\mathscr{B}_a = \{B_{a,b} | b \in N\}$, then*

(1) *$(N, \mathscr{B}_a)$ is a cyclic block design with parameters*

$$v = b = p^n \quad \text{and} \quad r = k = (p-1)^{-1}(p^{h+1}-1)t + (n-h-1)t + 1.$$

(2) *There exist $c = \frac{p-1}{t} p^{n-h-1}$ disjoint cyclic block designs $(N, \mathscr{B}_a)$, $a \in C$, isomorphic to each other.*

(1) Firstly, we note that $\mathscr{D}_a = (N, \mathscr{B}_a)$ is the development of the basic block $B_{a,0}$, so it is obviously cyclic. Proposition 3.5 tells us that $b = |N| = p^n$. We know that each block contains exactly $k = \frac{p^{h+1}-1}{p-1}t + (n-h-1)t + 1$ elements from Proposition 3.4. Finally, as the number of the blocks containing an element $x \in N$ equals the number of the blocks containing 0, obviously, we can say that each element of N occurs in the same number of blocks. Thus the replication number is $r = bk/v = k$.
(2) The first part of the statement follows by Propositions 3.2 and 3.6. Moreover, any two designs $\mathscr{D}_{a_1} = (N, \mathscr{B}_{a_1})$ and $\mathscr{D}_{a_2} = (N, \mathscr{B}_{a_2})$ are isomorphic via the automorphism $\gamma_{a_2 a_1^{-1}}$ of $\mathbb{Z}_{p^n}$.

Theorem 3.8. *Let N be a p^n-maximal wd-nearring with $|\Gamma(C)| = tp^h$ and $(t, p) = 1$. Set $\mathscr{B} = \{B_{a,b} \mid a \in C,\ b \in N\}$. Then $\mathscr{D} = (N, \mathscr{B})$ is a cyclic block design with parameters $v = p^n,\ b = cp^n,\ k = \frac{p^{h+1}-1}{p-1}t + (n-h-1)t + 1,\ r = ck$.*

We note that $\mathscr{D} = (N, \mathscr{B})$ results in the union of the $c = \frac{p-1}{t} p^{n-h-1}$ disjoint developments $\mathscr{D}_a = (N, \mathscr{B}_a)$, $a \in C$, and we apply Lemma 3.7.

In the sequel, block designs generated as in Section 3 will be called *block designs derived from N*.

4. PBIB-designs

Definition 4.1. An *association scheme with m associate classes* on a finite set N is a family $\mathscr{A}$ of m symmetric antireflexive binary relations $R_1, \ldots, R_m$ on N such that:

(i) any two distinct elements of N are ith associates for exactly one value of $i = 1, \ldots, m$;
(ii) for all $i = 1, \ldots, m$ and $x \in N$, there are exactly n_i distinct elements $y \in N$ 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 $z \in N$ such 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.

Definition 4.2. A tactical configuration $(N, \mathscr{B})$ is called a *balanced incomplete block design* (BIB-design) if there is a positive integer λ so that, if $x, y \in N$ are any two distinct elements of N, then there are exactly λ distinct blocks of $\mathscr{B}$ containing both x and y.

Definition 4.3. A tactical configuration $(N, \mathscr{B})$ with an association scheme $\mathscr{A}$ is called a *partially balanced incomplete block design* (PBIB-design) if there are positive integers λ_i, $i = 1, \ldots, m$, such that, if $x, y \in N$ are any two ith associate elements, then x, y occur together in exactly λ_i blocks of $\mathscr{B}$. Thus a PBIB-design $(N, \mathscr{B}, \mathscr{A})$ has parameters n_i, p_{ij}^k and λ_i in addition to those of the tactical configuration $(N, \mathscr{B})$.

Generally, the block designs derived from a p^n-maximal wd-nearring N are not *BIB*-designs. Nevertheless, we will see that it is possible to define an association scheme on N making them *PBIB*-designs. In order to obtain this, we recall the following constructions.

Construction 1. A block design $(N, \mathscr{B})$ is called an *orbital design* of Higman ([5, p. 162]) if we obtain $\mathscr{B}$ in the following way: take H a transitive permutation group with an intransitive subgroup S acting on a finite nonempty set N. Let B be any union of orbits of S and S_1 be the stabilizer of B, $|H : S_1| = b$. Choose the representatives x_i, $i = 1, \ldots, b$, for the cosets $x_i S_1$, $i = 1, \ldots, b$. Finally, set $\mathscr{B} = \{B_i = x_i(B),\ i = 1, \ldots, b\}$.

Construction 2. An orbital design $(N, \mathscr{B})$ can become a PBIB-design. Precisely, from [7] we know that from a transitive permutation group H of rank $f + 1$ on N, an orbital design can be derived which results in a PBIB-design with at most f associate classes determined as follows: consider a any element of N, H_a its stabilizer and $N = \{a\} \cup \Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_f$ the decomposition of N into the H_a-orbits. For each orbit Δ we have $\Delta' = \{g(a) | g \in H,\ a \in g(\Delta)\}$, which is again an orbit, of the same length as Δ, and $(\Delta')' = \Delta$. The orbits Δ and Δ' are called *paired* and an orbit is called *self-paired* if $\Delta = \Delta'$. Suppose Δ_i, $i = 1, \ldots, u$, are self-paired orbits and the remaining $f - u$ orbits Δ_i, Δ_i', $i = u + 1, \ldots, (f - u)/2$, are paired. Points a and b are said to be sth associates if $s \leqslant u$ and $b \in \Delta_s$ or $s > u$ and $b \in \Delta_s \cup \Delta_s'$. Moreover, $g(a)$ and $g(b)$, $g \in H$, are said to be sth associates if a and b are sth associates too. Finally, sth associate points occur together in λ_s blocks, where λ_s depends only on s.

Now, we come back to the block designs derived from a wd-nearring.

Lemma 4.4. *Let N be a p^n-maximal wd-nearring with $|\Gamma(C)| = tp^h$, $(t, p) = 1$. If $a \in C$ and $\mathscr{B}_a = \{B_{a,b} \mid b \in N\}$, then $(N, \mathscr{B}_a)$ is an orbital design.*

Take $\Phi = \Gamma(C)$ and consider $H = N \times_\sigma \Phi$, the natural semidirect product where $(a, \alpha) \times_\sigma (b, \beta) = (a + \alpha(b), \alpha\beta)$, which acts transitively on N by $(a, \phi)n = a + \phi(n)$. Consider $S = \{(0, \phi) \mid \phi \in \Phi\}$. S is a subgroup of H isomorphic to Φ, so $|H : S| = p^n$. Moreover, S acts intransitively on N, has the same orbits of Φ and turns out to be the stabilizer of $B_a = N * a$ in H, $a \in C$. From Proposition 3.4 we know that $N * a$ is a union of some Φ-orbits, so we can construct an orbital design following the method described previously. Denote by $\underline{m} = (m, id_N)$ the representative of the coset $\underline{m}S = \{(m, \phi) \mid \phi \in \Phi\}$. Let $\underline{0}, \ldots, \underline{p^n - 1}$ be the representatives of the cosets of S and compute $\underline{0}(B_a), \ldots, \underline{p^n - 1}(B_a)$: you find $\underline{b}(B_a) = B_{a,b}$, for all $b \in N$. Thus, $(N, \mathscr{B}_a)$ results in an orbital design.

Finally, we are able to prove the main theorem of this section.

Theorem 4.5. *Let N be a p^n-maximal wd-nearring with $|\Gamma(C)| = tp^h$ and $(t, p) = 1$. The block designs derived from N are* PBIB-*designs with either f associate classes, if t is even, or $f/2$ associate classes, if t is odd, where $f = [(ph - h + p)p^{n-h-1} - 1]/t$.*

Previous Lemma 4.4 tells us that $\mathscr{D}_a = (N, \mathscr{B}_a)$ is an orbital design; hence, applying Construction 2, an association scheme can be determined starting from the orbits of $\Phi = \Gamma(C)$ which makes $\mathscr{D}_a = (N, \mathscr{B}_a)$ a PBIB-design.

Actually, considering the group $H = N \times_\sigma \Phi$ of Lemma 4.4 acting transitively on N, we can identify the Φ-orbits with the orbits of the stabilizer of $0 \in N$, as $St(0) = \{(0, \phi) \mid \phi \in \Phi\}$ is isomorphic to Φ. Let f be the number of the nontrivial Φ-orbits. From Theorem 16.4 of [10] we learn that the paired orbits Δ and Δ' of Φ coincide if, and only if, there is an element $g \in H$ exchanging 0 and $x \in \Delta$. If $|\Phi|$ is even the element $g = (x, -id_N)$, exchanging 0 and x, exists in H, for all $x \in N$; thus, all the orbits are self-paired and the associate class number is f. If $|\Phi|$ is odd such an element does not exist in H, for all $x \in N$, so no nontrivial orbit is self-paired. Hence f is even and the associate class number is $f/2$. Using Proposition 3.3, we easily obtain that the number of the Φ-orbits covering $p^r\mathbb{Z}_{p^n} \setminus p^{r+1}\mathbb{Z}_{p^n}$ is $p^{n-h-1}(p-1)/t$, for $0 \leqslant r \leqslant h$, and $p^{n-r-1}(p-1)/t$, for $h < r \leqslant n-1$. So, $f = [(ph-h+p)p^{n-h-1} - 1]/t$.

Finally, the design $\mathscr{D} = (N, \mathscr{B})$, the union of the disjoint orbital designs $(N, \mathscr{B}_a)$, for $a \in C$ (Theorem 3.8), results in a PBIB-design with respect to the same association scheme.

4.1. Association scheme and partial balance parameters

In [8] we find many equalities involving PBIB-design parameters. For instance, for a PBIB-design we can define the $v \times b$ incidence matrix A and read all the values of λ_i in the elements of $A * A^{\mathrm{T}} = (c_{lm})$, $l \neq m$, where A^{T} denotes the transpose matrix of A. If, as usual, we say that each element is the 0th associate of itself we can write $p_{ii}^0 = n_i$ and $p_{i0}^k = p_{0i}^k = \delta_{ki}$ (the Kronecker delta) and we also know that the parameters of a PBIB-design with m associate classes satisfy $n_i = \sum_{u=0}^{m} p_{iu}^k$ and $n_k p_{ij}^k = n_i p_{kj}^i$. If the PBIB-design is derived from a p^n-maximal wd-nearring, further formulas for computing the PBIB-design parameters can be found.

In this section, $\mathscr{D} = (N, \mathscr{B})$ denotes a PBIB-design derived from a p^n-maximal wd-nearring, as described in the previous section. In the following $[B_{a,b} - B_{c,d}]$ denotes the list of the differences between the elements of $B_{a,b}$ and those of $B_{c,d}$. The number of times in which an element k occurs among the elements of $[B_{a,b} - B_{c,d}]$ is called the *frequency* of k in $[B_{a,b} - B_{c,d}]$. In particular the frequency of k in $[B_{a,0} - B_{c,0}]$ is denoted by $f_{a,c,k}$ and we set $f_{a,a,k} = f_{a,k}$.

Proposition 4.6. *The frequency of any $k \in N$ in $[B_{a,0} - B_{c,0}]$ equals the frequency of $\phi(k)$, that is, $f_{a,c,k} = f_{a,c,\phi(k)} \forall \phi \in \Phi$, $\forall a, c \in C$.*

Let $n \in N * a$ and $m \in N * c$. Obviously, when ϕ belongs to $\Phi \leqslant Aut(N^+)$, $\phi(n) \in N * a$ and $\phi(m) \in N * c$. Moreover, from $n - m = k$ we obtain $\phi(n) - \phi(m) = \phi(k)$ and vice versa.

Thus, to know all the possible frequencies of an element $k \in N$ in $[B_{a,0} - B_{c,0}]$ it is sufficient to know the frequency of any element of its orbit $\Phi(k)$.

Proposition 4.7. *The frequency of any $k \in N$ in $[B_{a,0} - B_{a,0}]$ equals the frequency of ka^{-1} in $[B_{1,0} - B_{1,0}]$, that is, $f_{a,k} = f_{1,ka^{-1}}\ \forall a \in C$.*

In fact $k \in [B_{a,0} - B_{a,0}]$ implies that there exist $z, t \in N$ such that $z * a - t * a = k$, that is, $a(z * 1 - t * 1) = k$ and finally $z * 1 - t * 1 = ka^{-1}$. The converse is analogous.

Remember that in a finite wd-nearring N the left translations determined by the elements of C form a subgroup $\Gamma(C) = \Phi$ of $Aut(N^+)$. For convenience, in the following E will denote a set of representatives, calling them e_i, of all the Φ-orbits contained in C, and D will denote a set of representatives, calling them d_i, of all the union sets $U_i = \Phi(d_i) \cup \Phi(-d_i) = \Delta_i \cup \Delta_i'$ of nontrivial Φ-orbits. On the basis of Section 3, if the Φ-orbits are self-paired, which means $|\Phi|$ is even, each of them is connected to an association class via $x R_i y$ if, and only if, $y - x \in \Phi(d_i) = \Delta_i$. If the Φ-orbits are not self-paired, which means $|\Phi|$ is odd, paired orbits are connected to an association class via $x R_i y$ if, and only if, $y - x \in \Phi(d_i) \cup \Phi(-d_i) = \Delta_i \cup \Delta_i'$.

Finally we are ready to prove the following.

Theorem 4.8. *Let $\mathscr{D} = (N, \mathscr{B})$ be a* PBIB*-design derived from a p^n-maximal wd-nearring. Then*

$$\lambda_i = \frac{1}{|\Phi|} \sum_{g \in C} f_{1,d_i g} = \sum_{e_j \in E} f_{1,d_i e_j}.$$

From Theorem 3.8 we know that $\mathscr{B} = \bigcup_{a \in C} \mathscr{B}_a$ and the number of distinct $\mathscr{B}_a$ is $c = \frac{p-1}{t} p^{n-h-1}$. Consequently $\lambda_i = \sum_{a \in E} (\lambda_i)_a$, where $(\lambda_i)_a$ denote the number of blocks of $\mathscr{B}_a$ containing two ith associate elements. From [8], Lemma 1 of Chapter 3, we learn that the number of blocks of $\mathscr{B}_a$ containing two given distinct elements x, y of N equals the frequency $f_{a,y-x}$ of $y - x$ in $[B_{a,0} - B_{a,0}]$. From Proposition 4.7 we know that $f_{a,y-x} = f_{1,(y-x)a^{-1}}$. Bearing in mind that two elements of C belong to the same orbit if, and only if, they generate the same basic block, the number of blocks containing x and y is $\frac{1}{|\Phi|} \sum_{g \in C} f_{1,(y-x)g}$. Now, choose x, y so that $x - y = d_i$, the representative of U_i. Obviously x and y are ith associates; thus, $\lambda_i = \frac{1}{|\Phi|} \sum_{g \in C} f_{1,d_i g}$. Instead of having g running in C, which forces the division by $|\Phi|$, we can choose a representative e_i in each orbit contained in C to obtain $\lambda_i = \sum_{e_j \in E} f_{1,d_i e_j}$.

Corollary 4.9. *Let $\mathscr{D} = (N, \mathscr{B})$ be a* PBIB*-design derived from a p^n-maximal wd-nearring. If $\Delta_i \subseteq C$ then $\lambda_i = \sum_{e_j \in E} f_{1,e_j}$ and if, moreover, the Φ-orbits are not self-paired, we obtain $\lambda_i = 2 \sum_{d_j \in D \cap C} f_{1,d_j}$.*

Theorem 4.10. *Let $\mathscr{D} = (N, \mathscr{B})$ be a* PBIB*-design derived from a p^n-maximal wd-nearring. Consider the three union sets $U_k = \Delta_k \cup \Delta_k'$, and $U_i = \Delta_i \cup \Delta_i'$, and $U_j = \Delta_j \cup \Delta_j'$. If two of them are contained in a proper subgroup N' of N^+ and the third has an empty intersection with N', then $p_{ij}^k = p_{kj}^i = p_{ik}^j = 0$.*

Let N' be a proper subgroup of N^+. Suppose $U_i, U_j \subseteq N'$ and $U_k \cap N' = \emptyset$. Consider the two kth associate elements 0 and d_k, the representative of U_k. The ith associates of

0 are the elements of U_i and the jth associates of d_k are the elements of $U_j + d_k$. Thus $p_{ij}^k = |U_i \cap (U_j + d_k)|$. Suppose $p_{ij}^k \neq 0$. Then there exists at least an element u belonging to $U_i \cap (U_j + d_k)$, that is, $u \in U_i$ and $u = d + d_k$ for some $d \in U_j$. Thus $d_k = u - d \in N'$ and this is excluded, as $U_k \cap N' = \emptyset$. From $p_{ij}^k = 0$ we obtain $p_{kj}^i = 0$, as $n_k p_{ij}^k = n_i p_{kj}^i$ and $n_i \neq 0$. For the same reason and bearing in mind that $p_{ij}^k = p_{ji}^k$, we have $p_{ik}^j = 0$.

Theorem 4.11. *In a* PBIB-*design* $\mathscr{D} = (N, \mathscr{B})$ *derived from a* p^n*-maximal wd-nearring, we have* $n_i = |\Delta_i|$ *if* $|\Phi|$ *is even, and* $n_i = 2|\Delta_i|$ *if* $|\Phi|$ *is odd.*

Obviously, the number n_i of ith associates of any $x \in N$ equals the cardinality of $U_i = \Delta_i \cup \Delta_i'$ and, from Theorem 4.5, we know that $\Delta_i = \Delta_i'$ if, and only if, $|\Phi|$ is even.

5. Example

In this section, we give the reader an example of the previous construction, developed in the following steps:

First step: *choose* G, Φ *and define* " $*$ " .
Second step: *construct block designs*.
Third step: *define an association scheme*.
Fourth step: *have PBIB-designs and their partial balance parameters*.

Example 5.1. First step: *choose* G, Φ *and define* " $*$ " .

We consider the additive group $G = (\mathbb{Z}_{7^3}, +)$ and we choose $\Phi \leqslant Aut(G)$ of order 21. So we are working with $p = 7$, $n = 3$, $t = 3$ and $h = 1$. We can compute the number of the Φ-orbits covering $C = \mathbb{Z}_{7^3} \setminus 7\mathbb{Z}_{7^3}$, $c = 14$ (see Proposition 3.2). Now we have to select a set E of the representatives of these Φ-orbits and, for convenience, we want that $1 \in E$. The Φ-orbits are not self-paired because the order of Φ is odd, so a suitable selection is $E = (e_j)_{j \in \{1,\ldots,14\}} = (1 + 7i, 342 - 7i)$ with $i = 0, \ldots, 6$. Now, from Theorem 2.5 we learn that a new multiplication " $*$ " can be defined on $\mathbb{Z}_{7^3}$. Actually, now we are not really interested in the whole construction of this multiplication, thus, we refer the interested reader to [1]. Anyway, now we know that a 7^3-maximal wd-nearring is generated.

Second step: *construct block designs*.

Using as blocks the sets $N * a + b$, with $a \in C$, $b \in N$, block designs can be generated. We have 14 basic blocks: $N * e_j$, for $j = 1, \ldots, 14$. Each of them generates a cyclic block design with parameters $v = b = 343$ and $k = r = 28$ (Theorem 3.7). So we have 14 cyclic block designs, isomorphic to each other, and their union is a cyclic block design with the following parameters.

$v = 343$, $b = 14 \cdot 343$, $k = 28$ and $r = 14 \cdot 28$.

Third step: *define an association scheme*.

We follow the construction described in Section 4. We can compute the number of the nontrivial Φ-orbits, $f = 30$ (see Theorem 4.5). As $|\Phi| = 21$ is odd, we know that the nontrivial 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 $i = 1, \ldots, 15$. Thus we obtain an association scheme with 15 associate classes defining x and y to be ith associates when $x - y$ belongs to U_i. To compute the parameters of our

association scheme we need the set D of the representatives of the U_is. A good selection could be $D = (d_i)_{i\in I_{15}} = (1, e_2, \ldots, e_7, 7, 7e_2, \ldots, 7e_7, 49)$.

We know that the number of the ith associates of each element depends on i only, and now we have $n_i = |U_i|$, and thus $n_1 = \cdots = n_7 = 42$, $n_8 = \cdots = n_{15} = 6$ (see Proposition 3.3).

Since $m = 15$, the p_{ij}^k fill in 15 squared matrices of order 15, the

$$P_k = \left(\begin{array}{ccc|ccc} p_{1\,1}^k & \cdots & p_{1\,7}^k & p_{1\,8}^k & \cdots & p_{1\,15}^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{7\,1}^k & \cdots & p_{7\,7}^k & p_{7\,8}^k & \cdots & p_{7\,15}^k \\ \hline p_{8\,1}^k & \cdots & p_{8\,7}^k & p_{8\,8}^k & \cdots & p_{8\,15}^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{15\,1}^k & \cdots & p_{15\,7}^k & p_{15\,8}^k & \cdots & p_{15\,15}^k \end{array}\right) = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & Q_4 \end{array}\right) \quad \text{for} \quad k = 1, \ldots, 15.$$

Theorem 4.10 gives us

$$P_k = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & 0 \end{array}\right) \text{ for } k = 1, \ldots, 7, \quad P_k = \left(\begin{array}{c|c} Q_1 & 0 \\ \hline 0 & Q_2 \end{array}\right) \text{ for } k = 8, \ldots, 15.$$

In addition we notice that p_{ij}^k equals the frequency of d_k, the representative of U_k, in the list of the differences between the elements of U_i and those of U_j.

Fourth step: *have PBIB-designs and their partial balance parameters*.

From Theorem 4.5, the constructed block design $\mathscr{D}$ with the previous association scheme turns out to be a PBIB-design which may be split into 14 orbital block designs, isomorphic to each other. To compute their parameters we apply Propositions 4.8 and 4.9 directly. For convenience, we will denote by $\mathscr{D}_j$ the orbital design generated by $B_{e_j,0} = N * e_j$, $j = 1, \ldots, 14$, and by $(\lambda_i)_j$, $i = 1, \ldots, 15$, the respective partial balance parameters. From Theorem 4.8 we know that $(\lambda_i)_j = (\lambda_i)_{e_j} = f_{1,e_j^{-1}d_i}$ and we notice that $(\lambda_i)_1 = (\lambda_i)_8$, $(\lambda_i)_2 = (\lambda_i)_9$, $(\lambda_i)_3 = (\lambda_i)_{10}$, $(\lambda_i)_4 = (\lambda_i)_{11}$, $(\lambda_i)_5 = (\lambda_i)_{12}$, $(\lambda_i)_6 = (\lambda_i)_{13}$, $(\lambda_i)_7 = (\lambda_i)_{14}$.

	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8	λ_9	λ_{10}	λ_{11}	λ_{12}	λ_{13}	λ_{14}	λ_{15}
$\mathscr{D}_1$	4	0	0	1	7	1	1	1	0	0	1	1	1	1	23
$\mathscr{D}_2$	1	4	0	0	1	7	1	1	1	0	0	1	1	1	23
$\mathscr{D}_3$	1	1	4	0	0	1	7	1	1	1	0	0	1	1	23
$\mathscr{D}_4$	7	1	1	4	0	0	1	1	1	1	1	0	0	1	23
$\mathscr{D}_5$	1	7	1	1	4	0	0	1	1	1	1	1	0	0	23
$\mathscr{D}_6$	0	1	7	1	1	4	0	0	1	1	1	1	1	0	23
$\mathscr{D}_7$	0	0	1	7	1	1	4	0	0	1	1	1	1	1	23
$\mathscr{D}$	28	28	28	28	28	28	28	10	10	10	10	10	10	10	322

References

[1] E. Aichinger, F. Binder, J. Ecker, P. Mayr, C. Nöbaner, SONATA—system of near-rings and their applications, Package for the group theory system GAP4, 2002.
[2] A. Benini, F. Morini, Weakly divisible nearrings on the group of integers (mod p^n), Riv. Mat. Univ. Parma 1 (6) (1998) 1–11.
[3] A. Benini, F. Morini, On the construction of a class of weakly divisible nearrings, Riv. Mat. Univ. Parma 1 (6) (1998) 103–111.
[4] A. Benini, S. Pellegrini, Weakly divisible nearrings, Discrete Math. 208/209 (1999) 49–59.
[5] J.R. Clay, Nearrings: Geneses and Applications, Oxford Science Publications, Oxford University Press, NY, 1992.
[6] G. Ferrero, Stems planari e BIB-Disegni, Riv. Mat. Univ. Parma 11 (2) (1970) 79–96.
[7] M. Hall, Designs with transitive automorphism group, in: T.L. Motzkin (Ed.), Proceedings of Symposia in Pure Math., American Mathematical Society, New York, 1971, pp. 109–113.
[8] A. Penfold Street, D.J. Street, Combinatorics of experimental design, Oxford Science Publication, Clarendon Press, 1987.
[9] G. Pilz, Near-rings, second ed., North Holland Math Studies 23, Amsterdam, 1983.
[10] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.