Generating Balanced Incomplete Block Designs from Planar Near Rings

JAMES R. CLAY

University of Arizona, Tucson, Arizona 85721

Communicated by A. Fröhlich

Received April 14, 1971

In [5], Ferrero demonstrates a connection between a restricted class of planar near rings and balanced incomplete block designs (BIBD). In particular, if the order \( v \) of an abelian group \((A, +)\) is relatively prime to 6, then Ferrero constructs a planar near ring \((A, +, \cdot)\) whose blocks \(Ag + h, g \neq 0\), are the blocks of a BIBD with parameters \((v, \beta, k, r, \lambda) = (v, v(v - 1)/2, 3, 3(v - 1)/2, 3)\). In this paper we show: (1) that the restrictions imposed by Ferrero on planar near rings can be relaxed, (2) the construction of two large family of BIBD's, and (3) that the additive group of a planar near ring need not be abelian in contrast to that of a planar near field [10].

Preliminaries

A near ring is a triple \((N, +, \cdot)\) such that \((N, +)\) is a group, \((N, \cdot)\) a semigroup, and \(\cdot\) is left distributive over \(+\). Elements \(a, b \in N\) are left equivalent multipliers if \(ax = bx\) for all \(x \in N\), and we write \(a \equiv m_b\). A near ring \(N\) is said to be planar if \(a \equiv m_b\) implies each equation

\[ ax = bx + c \]

has a unique solution for \(x\) in \(N\), and the equivalence relation \(\equiv_m\) yields at least three equivalence classes. If \(a \equiv_m 0\) implies \(a = 0\), then the planar near ring is said to be integral. Planar near rings were first studied in [1] and further geometric interpretations were given in [3, 5].

A balanced incomplete block design (BIBD) is a set \(B\) of \(v\) objects (sometimes called varieties) together with a family \(\mathcal{B}\) of \(\beta\) subsets of \(B\), called blocks, such that i) each block contains exactly \(k\) objects; ii) each object belongs to exactly \(r\) blocks; and iii) each pair of distinct objects belong to exactly \(\lambda\) blocks. The parameters satisfy the following equations:

\[ \beta k = vr, \quad r(k - 1) = \lambda(v - 1). \]
One can find more information on BIBD's and their applications to non-mathematical problems in [6, 7].

For a near ring \((N, +, \cdot)\), the subsets \(Na + b, a \neq 0\), are called blocks. These blocks give interesting geometric interpretations to planar near rings [1, 3, 5]. If a finite planar near ring \(N\) has no sub-near field, and if

\[ e(N) := \left| N/\equiv_m \right|, \]

the number of equivalence classes defined by \(\equiv_m\) on \(N\), is odd in cardinality, then Ferrero [5] shows that the blocks of \(N\) yield a BIBD with parameters

\[ (\beta, \beta(\beta - 1)/(\beta - 1), k, k(\beta - 1)/(\beta - 1), k) = (v, \beta, k, r, \lambda), \]

where \(v = |N|\) and \(k = e(N)\). The existence of such near rings are demonstrated for any abelian group \((A, +)\) with \(|A|, 6) = 1\). In these, \(k = 3\).

We will see that such restriction on \(N\) are not necessary.

**CONSTRUCTING BIBD's FROM FINITE FIELDS**

In [3], BIBD's are constructed from the prime fields \((\mathbb{Z}_p, +, \cdot), p \neq 2\), with parameters

\[ (p, p(p - 1)/(p - 1), k, k(p - 1)/(p - 1), k), \]

where \(k - 1\) is any nontrivial divisor of \(p - 1\). We will now show that these construction methods can be extended to any finite field. We will make use of the following

**THEOREM A.** For a finite field \((F, +, \cdot)\) of order \(p^n, p\) a prime, and for each nontrivial divisor \(t\) of \(p^n - 1\), there is an integral planar near ring \((F, +, \cdot)\).

**Proof.** We need only define \(*_t\), the rest being direct. Since \(F^* = F\setminus\{0\}\) is cyclic of order \(p^n - 1\), there is exactly one subgroup \(B\) of order \(t\) and index \(m\). Let \(Bu_1, Bu_2, ..., Bu_m\) be the cosets of \(B\) in \(F^*\) with fixed representatives \(u_i\), where \(u_1 = 1\). Define \(0 *_t a = 0\) for all \(a \in F\). If \(g \in F^*\), then \(g = b * u_i\) for some unique \(i\) and unique \(b \in B\). Define \(g *_t a = b \cdot a\).

Note that \(*_t\) depends not only upon \(t\) but on our choice of representatives \(u_i\); hence, there are many such integral planar near rings but they all yield the same blocks \(F *_t a + b = B \cdot a + b\), where \(B = B \cup \{0\}\).

Before stating and proving our main theorem, we give a couple of useful results of Ferrero together with a translation of his proofs (Lemma 11 and Lemma 16 of [5]).
**Lemma 1.** If blocks $Na + b$ and $Na' + b'$ of a planar near ring $(N, +, \cdot)$ coincide, then either (1) $b = b'$ and $Na = Na'$, or (2) $b \neq b'$ and the difference of two nonzero elements of $Na$ is an element of $N(-a)$ and $N(-a) = Na'$.

**Proof.** Suppose $b \neq b'$. Then there is a $g \in N$ such that $b = ga' + b'$, hence $b - b' = ga'$. Analogously, there is a $g' \in N$ such that $b' - b = g'a$. One then deduces that $b - b' \in Na' \cap N(-a)$ since $-(g'a) = g'(-a)$, and consequently, $Na' = N(-a)$.

We can now write $Na + b = N(-a) + b' = N(-a) + g'a + b$. Hence, $Na = N(-a) + g'a$. Multiplying from the left both sides of this equality by an appropriate $g^* \in N$ yields $Na = N(-a) + a$, and consequently repeating this for all $g \in N$ one gets $Na = N(-a) + c$ for all $c \in Na$. So if $0 \notin \{c_1, c_2\} \subseteq Na$, then $N(-a) + c_1 = N(-a) + c_2$ and hence $c_1 - c_2 \in N(-a)$.

**Lemma 2.** Suppose $N$ is a finite, integral, planar near ring with the property that $Na + b = Na' + b'$ implies $b = b'$. Then every pair of distinct elements of $N$ belong to exactly $k$ blocks where $k = e(N)$.

**Proof.** Suppose $x, y \in N$ and $x \neq y$. The three types of blocks possibly containing both $x$ and $y$ are of the form

(i) $Na + x$,
(ii) $Na + y$,
(iii) $Na + b$, $b \notin \{x, y\}$.

Certainly $x \in Na + x$; so suppose $y \in Na + x$. Then there is a $g \in N$ such that $y = ga + x$, and so $y - x \in Na$. One can show directly or use Theorem 1 of [1] that there is exactly one set $Na$ such that $y - x \in Na$, and consequently $x, y$ belong to exactly one block of the form $Na + x$. Similarly, for blocks of the form $Na + y$.

Now suppose $g \neq_m g'$. Since $N$ is planar, there is a unique $a \in N$ such that

$$g'(-a) = g(-a) + (x - y),$$

or equivalently

$$x - y = ga - g'a.$$ 

Since $(N, +)$ is a group, we have unique $b, b'$ satisfying

$$x = ga + b,$$
$$y = g'a + b'.$$

Hence

$$x - y = ga + b - b' - g'a$$
and

\[ x - y = ga - g'a. \]

Consequently, \( b = b' \). What we have seen is that for each pair \( g, g' \) such that \( g \equiv_m g' \) there is a unique pair \( a, b \) such that

\[ x, y \in Na + b. \]

Of these \((k - 1)(k - 2)\) pairs \( g, g', k - 1 = e(N) - 1 \) of them yield the same block for each such pair \( g, g' \). (This is because there are \( k - 1 \) terms \( a = a_1, a_2, \ldots, a_{k-1} \) such that \( Na_1 = Na_2 = \cdots = Na_{k-1} \), as can be seen directly, or is an easy consequence of Theorem 1 of [1].) Hence there are \( k - 2 \) blocks of the form \( Na + b, h \not\in \{x, y\} \), containing the elements \( x, y \). Together with the two from above, we have the desired number.

The condition that \( N \) be integral in the statement of Lemma 2 can be removed as seen by Theorem 3 of [5]. Here one must observe that a finite planar near ring can be made into an integral planar near ring by redefining the multiplication for the elements \( a = m 0 \) in accordance with Theorem 10 of [4]. In the new near ring, one gets the same blocks as with the old one. Hence the result of Lemma 2 remains valid.

We are now in a position to state and prove one of our main results

**Theorem B.** Suppose \((F, +, \ast)\) is any one of the integral planar near rings defined in Theorem A. Then:

1. \( t = p^n - 1 \) implies the blocks of \((F, +, \ast)\) give a BIBD with parameters
   
   \[ v = p^n, \quad \beta = p^n(p^n - 1)/p^m(p^m - 1), \quad r = (p^n - 1)/(p^m - 1), \quad k = p^m, \quad \lambda = 1; \]

2. \( t \neq p^n - 1 \) implies the blocks of \((F, +, \ast)\) give a BIBD with parameters
   
   \[ v = p^n, \quad \beta = p^n(p^n - 1)/t, \quad r = (t + 1)(p^n - 1)/t, \quad k = \lambda = t + 1. \]

**Proof.** Recall that the blocks \( F \ast \cdot a + b = \overline{B} \cdot a + b \), where \( B \) is the multiplicative subgroup of \( F^* = F - \{0\} \) of order \( t \) in the original field and \( \overline{B} = B \cup \{0\} \).

\(^1\) This theorem was proven concurrently by a student of the author, Richard H. Palmer.
Suppose \( Ba + b = Ba' + b' \) and \( b \neq b' \). We shall presently show that each \( Ba \triangleleft F^+ \). From \( Ba = Ba' + (b' - b) \), one gets \( Ba = B(b' - b) \) and, consequently,

\[
Ba(b' - b)^{-1} = B = Ba'(b' - b)^{-1} + 1.
\]

Now \( 0 \in B \) forces \( -1 \in Ba'(b' - b)^{-1} = B(-1) \), and we get

\[
B = B(-1) + 1.
\]

From Lemma 1, \( h, h' \in B \) implies \( h - h' \), \( h' - h \in B(-1) \). Note \( h \in B \) is equivalent to \( -h \in B(-1) \); so \( h' - h \in B \cap B(-1) \) which forces \( B = B(-1) \). From \( B = B + 1 \) we have

\[
B = B + h
\]

for all \( h \in B; \) so \( B \triangleleft F^+ \). It follows directly that each \( Ba \triangleleft F^+ \).

So from \( Ba + b = Ba' + b' \) one gets \( Ba = Ba' + (b' - b) \), and consequently \( Ba' + (b' - b) = Ba' = B, \) since \( Ba, Ba' \) are subgroups of \( F^+ \). In summary, \( Ba + b = Ba' + b' \) if and only if they are the same coset of the same subgroup \( B \) of \( F^+ \). (Hence \( t = p^n - 1 \), where \( m \mid n \).

Assume \( t = p^m - 1 \). Then \( B \triangleleft F^*, B \triangleleft F^+ \) implies \( (B, +, \cdot) \) is a subfield of \( (F, +, \cdot) \). Our “basic blocks” are

\[
B = Ba_1, Ba_2, ..., Ba_u,
\]

where \( u = (p^n - 1) \div t = (p^n - 1) \div (p^m - 1) \). Each \( Ba_i \) yields \( p^m/p^m \) blocks \( Ba_i + b_j \) since \( Ba_i \triangleleft F^+ \) is of index \( p^m/p^n \). Hence there are \( p^m(p^n - 1)/p^m(p^m - 1) \) distinct blocks in \( (F, +, \cdot) \).

Each block contains \( p^m \) objects. For each \( x \in F \) and for each \( Ba_i \) there is exactly one block \( Ba_i + b_j \) which contains \( x \). So \( x \) belongs to exactly \( r = (p^n - 1)/(p^m - 1) \) blocks.

Now let \( x, y \in F, x \neq y \) be chosen arbitrarily, and suppose

\[
x, y \in (Ba + b) \cap (Ba' + b').
\]

Then we get

\[
x' = x - b, \quad y' = y - b \in Ba \cap [Ba' + (b' - b)].
\]

Since \( Ba \triangleleft F^+ \), \( 0 \neq x' - y' \in B(-a) = Ba \) and one easily gets \( x' - y' \in Ba' \) also. But \( Ba \cap Ba' = \{0\} \) or else \( Ba = Ba' \). So we are forced to conclude that \( Ba + b = Ba' + b' \) and that there is at most one block \( Ba + b \) containing \( \{x, y\} \). Since \( \{x, y\} \subseteq B(x - y) + y \), we get exactly one block containing \( \{x, y\} \). Hence, \( \lambda = 1 \).
Now assume $t \neq p^n - 1$. With this restriction, the first part of the proof shows that the hypotheses of Lemma 2 are valid. This shows that $\lambda = k = t + 1$. Since we again have $(p^n - 1)/t$ “basic blocks”

$$\mathcal{B} = \mathcal{B}_a_1, \mathcal{B}_a_2, ..., \mathcal{B}_a_u$$

and each “basic block” yields $p^n$ distinct blocks, we calculate $\beta = \frac{p^n(p^n - 1)}{t}$ distinct blocks in $(F, +, \cdot)$. As above, we see each block contains $k = t + 1$ distinct objects.

We now calculate $r$. For a fixed “basic block” $\mathcal{B}_a_i$, as $b$ varies through $F$, a fixed element $x \in F$ will occur in $|\mathcal{B}_a_i| = t$ blocks $\mathcal{B}_a_i + b$. Hence $x$ is a member of $r = (t + 1)(p^n - 1)/t$ distinct blocks. This completes the proof of our theorem.

Note. The proof of this theorem shows that, for the case $t = p^n - 1$, the blocks $F \ast a + b$ are just the lines $y = ax + b$, $x \in B$, in the $n/m$-dimensional affine space $F$ over the subfield $(F, +, \cdot)$ of the field $(F, +, \cdot)$.

**CONSTRUCTING BIBD’S FROM FINITE ABELIAN GROUPS VIA NON-ABELIAN GROUPS**

In [8], B. H. Neuman gives an example of a nonabelian group $(N, +)$ of order $7^3$ with a fixed point free group of automorphisms. If $(\mathbb{Z}_7, +)$ denotes the integers modulo 7, this group is given by $N = \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, the cartesian product of sets, and

$$(a, b, c) \oplus (x, y, z) = (a + x, b + y, c + z + x \cdot y)$$

The automorphism

$$\alpha : (a, b, c) \rightarrow (2a, 2b, 4c)$$

yields $\Phi = \{1, \alpha, \alpha^2\}$, a fixed point free group of automorphisms of $(N, \oplus)$. Using the methods of Ferrero [4, 5] one can construct a planar near ring $(N, \oplus, \ast)$. Using the method described in this section, one can show that the blocks $N \ast a \oplus b$ of this planar near ring are the blocks of a balanced incomplete block design (BIBD). The purpose of this section is to generalize this example and, at the same time, obtain similar results.

Suppose $(A, +)$, $(B, +)$, and $(C, +)$ are abelian groups and let $N = A \times B \times C$ be the cartesian product of the underlying sets. Define $\oplus$ on $N$ by

$$(a, b, c) \oplus (x, y, z) = [a + x, b + y, c + z + \pi(x, b)]$$

where $\pi(x, b)$ denotes the projection of $x$ onto $B$. This defines a group operation on $N$ that is compatible with the group operations on $A$, $B$, and $C$. Using this operation, one can construct a balanced incomplete block design (BIBD) whose blocks are of the form $N \ast a \oplus b$. The purpose of this section is to generalize this example and, at the same time, obtain similar results.
where \( \pi : A \times B \to C \) is a mapping. It is direct to show that \( \oplus \) is associative if and only if
\[
\pi(s, b) + \pi(x, b + t) = \pi(x, t) + \pi(s + x, b)
\]
(4)
for all \( s, x \in A \) and for all \( b, t \in B \).

First letting \( x = 0 \) and then \( b = 0 \) in (4), one gets
\[
\pi(s, b) + \pi(0, b + t) = \pi(0, t) + \pi(s, b)
\]
or
\[
\pi(0, b + t) = \pi(0, t)
\]
for all \( b, t \in B \). Hence \( \pi(0, b) = \pi(0, 0) \) for all \( b \in B \). Similarly one gets \( \pi(a, 0) = \pi(0, 0) \) for all \( a \in A \). In summary,
\[
\pi(a, 0) = \pi(0, 0) = \pi(0, b)
\]
(5)
for all \( a \in A \) and for all \( b \in B \).

Setting \( s = 0 \) in (4) and then \( t = 0 \) in (4), one gets
\[
\pi(x, b + t) = \pi(x, b) + \pi(x, t) - \pi(0, 0)
\]
\[
\pi(s + x, b) = \pi(s, b) + \pi(x, b) - \pi(0, 0).
\]
(6)
Hence \( \pi(0, 0) \) measures the deviation of \( \pi \) from being bilinear; i.e., \( \pi = f + \pi(0, 0) \) where \( f : A \times B \to C \) is bilinear. Conversely, if \( f : A \times B \to C \) is bilinear, \( c \in C \) is a constant, and \( \pi : A \times B \to C \) is defined by \( \pi(a, b) = f(a, b) + c \), then \( \pi \) satisfies the identity of (4). We, consequently, have
\[
\pi(-s, b) = \pi(s, -b)
\]
(7)
for all \( s \in A \) and all \( b \in B \).

Using (5) and (7) one shows that \( (0, 0, -\pi(0, 0)) \) is an identity for \( \oplus \) and that \( (-a, -b, \pi(0, 0) - c + \pi(a, b)) \) is an inverse for \( (a, b, c) \). Hence \( (N, \oplus) \) is a group if and only if (4) is satisfied. The group \( (N, \oplus) \) is abelian if and only if \( \pi \) is a constant mapping.

The constant term \( \pi(0, 0) \) does not really give us anything more, for if \( \pi_1 = f \) and \( \pi_2 = f + c \) where \( f : A \times B \to C \) is bilinear and \( c \in C \) is a constant, then the map \( (x, y, z) \to (x, y, z - c) \) gives an isomorphism from the group \( (N, \oplus_1) \) defined by \( \pi_1 \) onto the group \( (N, \oplus_2) \) defined by \( \pi_2 \). So we may assume, without loss of generality, that \( \pi \) is bilinear. Summarizing to this point we have
Proposition C. For abelian groups $A, B, C$ and a mapping $\pi : A \times B \to C$, define $\oplus$ on $N = A \times B \times C$ by Eq. (3). The following are equivalent:

(i) $(N, \oplus)$ is a group;
(ii) $(N, \oplus)$ is a monoid;
(iii) $(N, \oplus)$ is a semigroup;
(iv) the identity (4) is valid;
(v) $\pi = f + c$ where $f : A \times B \to C$ is bilinear and $c \in C$ is a constant.

Moreover, $(N, \oplus)$ is an abelian group if and only if $\pi$ is a constant mapping; and $\pi_1 = f + c_1$, $\pi_2 = f + c_2$ define isomorphic groups if $f : A \times B \to C$ is bilinear and $c_1, c_2 \in C$ are constants.

We now turn our attention to the groups $(N, \oplus)$ defined by bilinear maps $\pi : A \times B \to C$. For our purposes it is useful to note that the center of such a group $(N, \oplus)$ is given by

$$Z(N, \oplus) = \{(a, b, c) \mid c \in C \text{ and } \pi(a, -) \text{ and } \pi(-, b) \text{ are zero morphisms}\}.$$ 

In any event, $C = \{(0, 0, c) \mid c \in C\} \subseteq Z(N, \oplus)$ and $C$ is isomorphic to $C$. Hence we have an exact sequence

$$0 \to C \to N \to N/C \to 0. \quad (8)$$

One can show directly that $N/C$ is isomorphic to the direct sum $A \oplus B$; so we can write (8) as

$$0 \to C \to N \to A \oplus B \to 0 \quad (8)'$$

which says that $N$ is a central extension of $C$ by $A \oplus B$ and hence $N$ is nilpotent of class 2.

In what follows, most of the notation and terminology for group theory is that used by Rotman in [9].

From (8), if we define $l((a, b, c) + \bar{C}) = (a, b, 0)$ as our lifting, the corresponding factor set

$$f : N/C \times N/C \to C$$

is given by

$$f((a, b, c) + \bar{C}, (x, y, z) + \bar{C}) = l((a, b, c) + \bar{C}) + l((x, y, z) + \bar{C}) - l([(a, b, c) + \bar{C}] - [(x, y, z) + \bar{C}])$$

which reduces to

$$f((a, b, c) + \bar{C}, (x, y, z) + \bar{C}) = (0, 0, \pi(x, b)). \quad (9)$$
(Since our extension (8) is central, it realizes the trivial morphism \( \theta : N/C \to \text{Aut } \tilde{C} \).) Conversely, one can verify directly that for any bilinear form \( \pi : A \times B \to C \) the mapping defined by (9) is a factor set for the corresponding extension of \( \tilde{C} \) by \( N/C \) given in (8).

Suppose \( \pi, \pi' \) define \( \oplus, \oplus' \), respectively, and that \((N, \oplus)\) and \((N, \oplus')\) are equivalent extensions of \( C \) by \( N/C \), and that both extensions realize the trivial morphism \( \theta : N/C \to \text{Aut } \tilde{C} \). Since \( \theta \) is trivial, there is a function \( \alpha : A \oplus B \to C \) such that

\[
(\pi - \pi')(x, b) = \alpha(x, y) - \alpha(a + x, b + y) + \alpha(a, b)
\]  

for all \( a \in A \) and all \( y \in B \). In particular, we can write

\[
(\pi - \pi')(a, y) = \alpha(a, b) - \alpha(a + x, b + y) + \alpha(x, y).
\]

Hence

\[
(\pi - \pi')(x, b) = (\pi - \pi')(a, y)
\]

for all \( x, a \in A \) and all \( b, y \in B \). In particular, we can choose \( a = 0 \) which yields, since \( \pi - \pi' \) is bilinear, \( \pi = \pi' \). Hence, we get an injection of \( \text{Hom}(A \otimes B, C) \) into the second cohomology group \( H_0^2(A \oplus B, C) \) since each bilinear \( \pi : A \times B \to C \) can be uniquely identified with an element of \( \text{Hom}(A \otimes B, C) \) and conversely. Summarizing we have

**Proposition D.** Let \( \pi : A \times B \to C \) be bilinear and suppose \( \oplus \) is defined by (3). Then

(i) \((N, \oplus)\) is a central extension of \( C \) by \( A \oplus B \); and

(ii) If \( \pi \neq \pi' \) and \( \pi' : A \times B \to C \) is also bilinear, then \( \pi \) and \( \pi' \) define nonequivalent extensions of \( C \) by \( A \oplus B \). Hence there is a natural embedding of \( \text{Hom}(A \otimes B, C) \) into the second cohomology group \( H_0^2(A \oplus B, C) \) defining the nonequivalent extensions of \( C \) by \( A \oplus B \) that realize the trivial morphism from \( A \oplus B \) into \( \text{Aut } C \).

Our next goal is to define a fixed-point free group of automorphisms of \((N, \oplus)\), where \( \oplus \) is given by some fixed but arbitrarily bilinear form, say \( \pi \). Keeping an eye on the example of Neumann at the beginning of this section, let \( A = \text{Aut } A \), \( B = \text{Aut } B \), and \( C = \text{Aut } C \). Then choose \( \alpha \in A \), \( \beta \in B \), \( \gamma \in C \) and define \( T : N \to N \) by

\[
T(a, b, c) = (\alpha a, \beta b, \gamma c).
\]

For \( T \) to be an automorphism, it is necessary and sufficient that

\[
\pi \circ \alpha \times \beta = \gamma \circ \pi;
\]
so \(\gamma\) does depend upon \(\alpha\) and \(\beta\). Let \([T], [\alpha], [\beta], [\gamma]\) be the cyclic groups generated by \(T, \alpha, \beta, \gamma\), respectively (assuming of course that \(\gamma\) satisfies (12)). One easily shows that \([T]\) is fixed-point free if and only if \([\alpha], [\beta], [\gamma]\) are all fixed-point free and each is isomorphic to \([T]\).

We shall now turn our attention to constructing BIBD from some of the groups \((N, \oplus)\). First, assuming (12) is satisfied, we wish to construct a planar near ring \((N, 0, *)\). If we have \([T]\) as a fixed-point free group of automorphisms of \((N, \oplus)\) we can, using the methods of Ferrero [4, 5], construct numerous planar near rings. Let

\[
\{0\}, a_{1}^{[T]}, a_{2}^{[T]}, \ldots, a_{k}^{[T]}, \ldots
\]  

be the orbits of \([T]\) acting on \(N\), where \(a_{i} \neq 0\) is a fixed but arbitrary representative of \(a_{i}^{[T]}\). Set \(0 * b = 0\) for all \(b \in N\). For \(a \neq 0\), there is a unique \(a_{i}\), such that \(a = a_{i}^{[T]}\); hence there is a unique \(\phi \in [T]\) such that \(\phi(a_{i}) = a\). If we set \(a * b = \phi(b)\), then one can see directly or refer to Theorem 10 of [4] and Theorem 3 of [5] that \((N, \oplus, *)\) is a planar near ring. Even though \(*\) depends heavily upon the choice of the \(a_{i}\), the resulting blocks \(N * a + b\) are independent of the choice of the \(a_{i}\), since \(N * a \ominus b = a^{[T]} \cup \{0\} \ominus b\). It is of interest to note that different choices of the \(a_{i}\) can lead to nonisomorphic planar near rings even though they all yield the same blocks (see Examples 22 and 24 of 2.6 in [3]).

We want to apply Lemmas 1 and 2. To this end, assume \(A, B, C\) are finite and none of these groups is an elementary 2-group. Suppose that \([T]\) is fixed-point free and that \(\gamma\) satisfies (12). For a planar near ring \((N, \oplus, *)\) defined by a \(\pi\) and \([T]\), we consider the blocks \(N * a \ominus b\), and apply Lemma 1. Note that if \(a = (a_{1}, b_{1}, c_{1})\), then

\[
N * a = \{(0, 0, 0), (a_{1}, b_{1}, c_{1}), (\alpha a_{1}, \beta b_{1}, \gamma c_{1}), \ldots, (\alpha^{q-1} a_{1}, \beta^{q-1} b_{1}, \gamma^{q-1} c_{1})\}
\]

and

\[
N * (-a) = \{(0, 0, 0), (-a_{1}, -b_{1}, \pi(a_{1}, b_{1}) - c), \ldots, (-\alpha^{q-1} a_{1}, -\beta^{q-1} b_{1}, \gamma^{q-1}(\pi(a_{1}, b_{1}) - c))\}
\]

if the order of \([T]\) is \(q\). Take \(x = (a_{1}, b_{1}, c_{1}), y = (\alpha a_{1}, \beta b_{1}, \gamma c_{1})\) in \(N * a\). Then

\[
x - y = (a_{1} - \alpha a_{1}, b_{1} - \beta b_{1}, c_{1} - \gamma c_{1} + \pi(\alpha a_{1}, \beta b_{1}) + \pi(-\alpha a_{1}, b_{1}))
\]

and

\[
y - x = (\alpha a_{1} - a_{1}, \beta b_{1} - b_{1}, \gamma c_{1} - c_{1} + \pi(a_{1}, b_{1}) + \pi(-a_{1}, b_{1}))
\]

are in \(N * (-a)\).
If $a_1 \neq 0$ or $b_1 \neq 0$, say, $a_1 \neq 0$, for example, then there are integers $l$, $k$ such that $l, k \in \{1, 2, \ldots, q - 1\}$ and

$$a_1 - \alpha a_1 = -\alpha^k a_1, \quad \alpha a_1 - a_1 = -\alpha^l a_1.$$ 

Adding, we get $0 = \alpha^l + \alpha^k = \alpha^k(1 + \alpha^{l-k})$. Hence $\alpha^{l-k} = -1$. If $l = k$, then $A$ would be an elementary $2$-group. Our only other choice is for $q$ to divide $2(l - k)$ which cannot be if we ensure that $2 \nmid q$.

Now suppose $a = 0$ and $b = 0$. Then

$$x - y = (0, 0, c - \gamma c)$$

and

$$y - x = (0, 0, \gamma c - c).$$

The above argument gives a contradiction in this case also. So, by Lemma 1, $N^*a \oplus b = N^*a' \oplus b'$ if and only if $b = b'$ and $N^*a = N^*a'$. Applying Lemma 2 shows that there are exactly $\lambda = e(N) = q + 1$ distinct blocks containing an arbitrary pair of distinct elements of $N$.

Each block contains exactly $k = q + 1 = \lambda$ elements. If $v = |A| |B| |C| = |N|$, then there are $(v - 1)/q = \omega$ distinct “basic blocks”

$$N^*a_1, N^*a_2, \ldots, N^*a_\omega,$$

one for each orbit of $[T]$. Each “basic block” $N^*a_i$ gives $\omega$ distinct blocks (again using Lemma 1), and so we get $\beta = \omega(v - 1)/q$ distinct blocks altogether.

Each “basic block” $N^*a_i$ contains exactly $q + 1$ elements. So, as $b$ varies through $N$, there will be exactly $q + 1$ blocks $N^*a_i \oplus b$ containing a fixed but arbitrary element $u \in N$. Consequently, $u$ belongs to exactly

$$r = (q + 1)(v - 1)/q$$

distinct blocks of $N$. Summarizing, we have

**Theorem E.** Let $(N, \oplus)$ be as in Proposition C, and suppose $\alpha, \beta, \gamma,$ and $T$ are as in (11). Then

(i) $T$ is an automorphism of $N$ if and only if $\pi \circ \alpha \times \beta = \gamma \circ \pi$;

(ii) $[T]$ is fixed-point free on $(N, \oplus)$ if and only if $[\alpha], [\beta], [\gamma]$ are fixed-point free on $A, B, C$, respectively, and each is isomorphic to $[T]$ as groups;

(iii) if $[T]$ is fixed-point free on $(N, \oplus)$, then each choice of representatives of the orbits of $[T]$ yields a planar near ring $(N, \oplus, \ast)$, where $\ast$ is defined as in the paragraph of (13);
(iv) if \((N, \oplus, \ast)\) is any of the planar near rings of (iii), \(N\) is finite, \(q\), the order of \([T]\), is odd, and none of the groups \(A, B, C\) is elementary 2-abelian, then the blocks \(N^*a + b\) of \(N\) form a BIBD with parameters

\[
v = |N|, \quad \beta = \frac{v(v - 1)}{q}, \quad k = \lambda = q + 1, \quad r = (q + 1)(v - 1)/q.\]

To see that the above results have a wider application than the example of Neumann, from which the theory was derived, the following lemma will be useful.

**Lemma 3.** Suppose \(R\) is a finite commutative ring with identity, and let \(t \neq 1\) be an element of the group of units \(U(R)\) of \(R\). Define \(\alpha : R \to R\) by \(\alpha(r) = tr\). Then \(\alpha\) is an automorphism of \(R^+\) and \([\alpha]\) is fixed-point free on \(R^+\) of order \(q\) if and only if \(t^k - 1\) is not a zero divisor in \(R\) for all divisors \(k\) of \(q\) different from \(q\).

**Proof.** It is trivial that \(\alpha\) is an automorphism of \(R^+\). Suppose \([\alpha]\) is fixed-point free. If \(t^k - 1\) is a zero divisor, then \(0 = (t^k - 1)a\) for some \(a \in R, a \neq 0\). Hence \(\alpha^k a = a\). Hence \(k = q\).

Conversely, \(\alpha^k a - a\) implies \((t^k - 1)a = 0\). Let \(k\) be the least positive integer with this property. Then using the division algorithm one can deduce that \(k | q\).

As an application, let \(R\) be as in Lemma 3. Let \(A = B = R^+ \oplus \cdots \oplus R^1\), a direct sum of \(n\) copies of \(R^+\), and define \(\tilde{\alpha} : A \to A, \tilde{\beta} : B \to B\) by \(\tilde{\alpha}(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n), \tilde{\beta}(b_1, \ldots, b_n) = (\beta b_1, \ldots, \beta b_n)\), where \(\alpha, \beta \in U(R)\) have the properties of the \(t\) in Lemma 3. Let \(C = R^+\) and define \(\gamma : C \to C\) by \(\gamma(c) = \alpha \beta c\). For \(\pi : A \times B \to C\) we take the inner product

\[
\pi[(a_1, \ldots, a_n), (b_1, \ldots, b_n)] = a_1 b_1 + \cdots + a_n b_n.
\]

Since \(\pi\) is bilinear, the corresponding \(\oplus\) on \(N = A \times B \times C\) gives a non-abelian group \((N, \oplus)\). To see that \(T(a, b, c) = (\tilde{\alpha} a, \beta b, \gamma c)\) defines an automorphism, we must show that \(\pi \circ \tilde{\alpha} \times \beta = \gamma \circ \pi\). Now

\[
\gamma \circ \pi[(a_1, \ldots, a_n), (b_1, \ldots, b_n)] = \gamma(a_1 b_1 + \cdots + a_n b_n)
\]

\[
= \alpha \beta (a_1 b_1 + \cdots + a_n b_n)
\]

and

\[
\pi \circ \tilde{\alpha} \times \beta[(a_1, \ldots, a_n), (b_1, \ldots, b_n)]
\]

\[
= \pi[(\alpha a_1, \ldots, \alpha a_n), (\beta b_1, \ldots, \beta b_n)]
\]

\[
= \pi[(\alpha a_1, \ldots, \alpha a_n), (\beta b_1, \ldots, \beta b_n)]
\]

\[
= \alpha \beta (a_1 b_1 + \cdots + a_n b_n).
\]
Hence $T$ is an automorphism. To get $[T]$ to act fixed-point free, we must have $[T] \cong [\bar{x}] \cong [\bar{y}] \cong [\gamma]$, and $[\bar{x}]$, $[\bar{y}]$, $[\gamma]$ to act fixed-point free. Since $\gamma$ is given in terms of $\alpha$ and $\beta$, we note that we cannot let $\alpha^k \beta^k - 1$ be a zero divisor in $R$. A sufficient condition to ensure this is that the multiplicative order of $\alpha \beta$ in $U(R)$ to be odd in addition to the restrictions already placed upon $\alpha$ and $\beta$. (There are certainly many finite fields for which such $\alpha$ and $\beta$ can be found.) With this further restriction we can be assured that $[\gamma]$ acts fixed-point free on $C$; hence $T$ will act fixed-point free.

The additional restriction that $R$ is not of characteristic 2 will now give us numerous examples of BIBD's illustrating the results of this section.

ACKNOWLEDGMENT

The author owes a debt of gratitude to Prof. A. Fröhlich for several suggestions which led to substantial improvements in this work.

REFERENCES

8. B. H. NEUMAN, Groups with automorphisms that leave only the neutral element fixed, Arch. Math. (Basel) 7 (1956), 1–5.