TAIWANESE JOURNAL OF MATHEMATICS
Vol. 14, No. 5, pp. 1713-1739, October 2010
This paper is available online at http://www.tjm.nsysu.edu.tw/

FROM PLANAR NEARRINGS TO GENERATING BLOCKS

Hsin-Min Sun

Abstract. Planar nearrings, like most of the subjects in finite geometries, can be applied for the construction of block designs. In this article we introduce the ideas of constructing simple BIBDs (balanced incomplete block designs) from field-generated (or nearfield-generated) planar nearrings. Further investigation reveals that there are strong connections between these kinds of constructions and the action of a sharply 2-transitive group on a set. We next explore the structures of the constructions. The theory is derived from finite fields directly. The main point is on finding a subset S (called generating block) of the field F with respect to the given stabilizer $Stab_{F^*}(S)$. A big portion of simple BIBDs with various parameters can be obtained in this way; many simple BIBDs with the same parameters appear. We classify the constructed BIBDs according to the types of the respective generating blocks.

1. Introduction

Planar nearring is one of the topics in finite geometries. M. Anshel and J.R. Clay began its study in the 1960s [1, 2]. In the 1980s, J. R. Clay got the idea of circles in a planar nearring [9, 11, 13]. Later on, he developed some related ideas about "rays", "line segments", and "lines" in a planar nearring [14]. The interested reader is referred to some materials [3, 10, 12, 17, 19, 20, 21] on planar nearrings and finite geometries. Especially there is a recent survey by W.-F. Ke [18].

Like most of the subjects in finite geometries (e.g., affine planes or projective planes), planar nearrings can be applied for the construction of block designs. The use of planar nearrings to constructing BIBDs dates back to Ferrero's and Clay's papers [8, 15]. J. R. Clay and his followers discover many related connections with these kinds of combinatorial structures and with other kinds.

In this article we will develop a method for constructing BIBDs from finite fields. This method covers all the results of constructing BIBDs from field-generated

Received June 22, 2007, accepted January 10, 2009.
Communicated by Wen-Fong Ke.
2000 *Mathematics Subject Classification*: Primary 12E20; Secondary 05B05, 12K05, 16Y30.
Key words and phrases: Finite field, Balanced incomplete block design, Difference family, Planar nearring.

planar nearrings. Structures of the constructions will be analyzed and the constructed BIBDs will be classified.

1.1. Planar Nearrings

A (left) *nearring* is an algebraic structure $(N, +, \cdot)$ such that $(N, +)$ is a group (not necessarily abelian), $(N, \cdot)$ is a semigroup (i.e., $\cdot$ is associative), and $\cdot$ satisfies the left distributive law with respect to $+$: $a\cdot(b+c) = a\cdot b+a\cdot c$, for any a, b, and c in N. The definition of planarity is motivated by two nonparallel lines intersecting at exact one point in affine planes constructed from fields. For a nearring $(N, +, \cdot)$, define an equivalence relation $=_m$ on N by $a =_m b$ if and only if $ax = bx$ for all $x \in N$. If $a =_m b$, we say that a and b are *equivalent multipliers*. A nearring $(N, +, \cdot)$ is called *planar* when (1) $=_m$ has at least three equivalence classes, i.e., $|N/{=_m}| \geq 3$; (2) for constants a, b, $c \in N$ with $a \neq_m b$, the equation $ax = bx + c$ has a unique solution for x in N.

The construction of planar nearrings is known as the *Ferrero Planar Nearring Factory* in Clay's book [12, §4]. We will not use the construction in the sequel. However, we need the definition of a Ferrero pair.

Definition 1.1. Let $(N, +)$ be a group, and let $Aut(N, +)$ be the set of all automorphisms of $(N, +)$. Let $\Phi \leq Aut(N, +)$ such that:

(1) $1_N \neq \phi \in \Phi$ and $\phi(x) = x$ implies $x = 0$ (i.e., Φ is a regular group of automorphisms).

(2) $-\phi + 1_N$ is surjective for any $1_N \neq \phi \in \Phi$.

We call (N, Φ) a *Ferrero pair*.

Note that every planar nearring is constructible from a Ferrero pair. And, if $(N, +, \cdot)$ is a planar nearring constructed from the Ferrero pair (N, Φ), then we have $N^* \cdot a = \Phi(a)$.

Let F be a field. Define automorphism $\phi_a : F \to F$ by $\phi_a(x) = ax$. Let P be a subgrooup of $(F^*, \cdot)$, $\Phi = \{\phi_a \mid a \in P\}$. Then (F, Φ) is a *field-generated Ferrero pair*. A planar nearring is *field-generated* if it is generated from a field-generated Ferrero pair. Similarly, there are nearfield-generated and ring-generated planar nearrings.

Let $(\mathbf{C}, +, \cdot)$ be the field of complex numbers. Define the operation $\circ$ on the complex plane $(\mathbf{C}, +, \cdot)$ by

$$a \circ b = \begin{cases} 0, & \text{if } a = 0; \\ \dfrac{a}{|a|} \cdot b, & \text{otherwise.} \end{cases}$$

Then $(\mathbf{C}, +, \circ)$ is a (left) planar nearring. Define the operation $*$ on the complex plane $(\mathbf{C}, +, \cdot)$ by

$$a * b = |a| \cdot b.$$

Then $(\mathbf{C}, +, *)$ is also a (left) planar nearring. These two planar nearrings, which are related to circles and rays in the complex plane, motivate some ideas in the study of geometry in finite planar nearrings.

Given a finite planar nearring $(N, +, \cdot)$, let $N^* = N \setminus \{0\}$. For $a, b \in N$, $a \neq 0$, the *circle* $C(a, b)$ with radius $|a|$ and centered at b is $N^* \cdot a + b$. For $a, b \in N$, $a \neq b$, the *ray* from a through b is $\overrightarrow{a, b} = N \cdot (b - a) + a$; the (*line*) *segment* with endpoints a and b is

$$\overline{a, b} = \overrightarrow{a, b} \cap \overrightarrow{b, a} = [N \cdot (b - a) + a] \cap [N \cdot (a - b) + b];$$

the *line* through a and b is

$$\overleftrightarrow{a, b} = \overrightarrow{a, b} \cup \overrightarrow{b, a} = [N \cdot (b - a) + a] \cup [N \cdot (a - b) + b].$$

Thus in finite geometries we are interested in knowing what kind of geometric properties these objects can possess.

1.2. Balanced Incomplete Block Designs (BIBDs)

Let V be a finite nonempty set of symbols, and suppose $\mathcal{B}$ is a nonempty collection of nonempty subsets of V. Then $(V, \mathcal{B})$ is called a *BIBD* (*balanced incomplete block design*) if there are parameters r, k, and λ with the following properties: every *block* in $\mathcal{B}$ has exactly k symbols; every symbol appears in exactly r blocks; every pair of distinct symbols appears in exactly λ blocks. There are another two parameters $v = |V|$ and $b = |\mathcal{B}|$. So sometimes a BIBD is described as a (v, b, r, k, λ) design. It is well-known that $vr = bk$ and $\lambda(v-1) = r(k-1)$. Therefore, once we know (v, k, λ) for a BIBD, the other two parameters are determined. Thus a BIBD is called a (v, k, λ) design. A design without repeated blocks is called *simple*. In this article we shall always consider simple BIBDs.

The modern study of BIBDs begins with Bose, Fisher, and Yates [6, 16, 24]. BIBDs can be constructed by various ways [5]. One of the methods uses difference families. Suppose $(V, +)$ is a group of order v. Let $B_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,k}\}$ $(1 \leq i \leq t)$ be t k-subsets of V. Then the collection $\{B_1, \ldots, B_t\}$ forms a (v, k, λ) *difference family* if every nonzero element of V appears exactly λ times in the list of differences $b_{i,j} - b_{i,l}$ $(1 \leq i \leq t;\ 1 \leq j, l \leq k)$. In this case, the B_i are called *base blocks* and all the translates of the base blocks form a (v, k, λ) BIBD. A k-subset S of V is a *short block* if $S + g = S$ for some nonzero $g \in V$. A collection of k-subsets of V forms a (v, k, λ) *partial difference family* if all the distinct translates of the *base blocks* form a (v, k, λ) BIBD.

Let v, k, and λ be positive integers. It is not difficult to check that (1) $\lambda(v-1) \equiv 0 \mod (k-1)$ and (2) $\lambda v(v-1) \equiv 0 \mod k(k-1)$ are necessary conditions for the existence of a BIBD with parameters (v, k, λ). We fix v and k, then the smallest positive integer that satisfies these conditions is denoted by λ_{min}. It then follows that λ_{min} divides λ whenever a (v, k, λ) BIBD exists. Let $\lambda_1 = (k-1)/\gcd(k-1, v-1)$ and let $\lambda_2 = k(k-1)/\gcd(k(k-1), v(v-1))$, then $\lambda_{min} = \mathrm{lcm}(\lambda_1, \lambda_2) = k(k-1)/c_1c_2\gcd(k, v)$ where $c_1 = \gcd(k, v-1)$ and $c_2 = \gcd(k-1, v-1)$.

Given a finite planar nearring $(N, +, \cdot)$ constructed from the Ferrero pair (N, Φ), let $\mathcal{B}^\circ = \{N^* \cdot a + b \mid a, b \in N, a \neq 0\}$ be the collection of circles. Clay shows that $(N, \mathcal{B}^\circ)$ is a BIBD [12, (5.5)] with parameters $v = |N|$, $b = v(v-1)/k$, $r = v-1$, $k = |N^*/{=_m}| = |\Phi|$, and $\lambda = k-1$. In particular, a circular planar nearring can produce a nice circular BIBD, in which any two distinct blocks have no more than two points in common. Sometimes, the collection of rays is also a BIBD [12, (7.9),(7.11)]. The author finds that segments [21] and lines in a field-generated (or nearfield-generated) planar nearring can be used to constructing BIBDs [20, (8.3), (8.5), (11.16)].

Investigations reveal that there are strong connections between these constructions and the action of a sharply 2-transitive group on a set. It is known that the action of a sharply 2-transitive group on a set yields a simple BIBD [5, III.4.6]. The *affine group* of a nearfield $(F, +, \cdot)$ is defined as

$$Aff(F) = \{\tau_{b,a} : F \to F \mid \tau_{b,a}(x) = bx + a,\, b \in F^*,\, a \in F\}.$$

We also know that $Aff(F)$ is a sharply 2-transitive group on F. Therefore, given any subset S of F, the orbit $Orb_G(S)$ of S under the action of $G = Aff(F)$ is a simple BIBD. In this article we explore the structures of these constructions.

To give a more transparent (and elementary) development, we derive the theory by using finite fields directly. In the next section, we introduce the method and analyze the basic structures. In section three, we give the constructions from finite fields. We will first show that there exists a subset S (called generating block) of the field F with respect to the given stabilizer $Stab_{F^*}(S)$. Accordingly, various BIBDs with the possible parameters can be obtained. Thereafter, we develop other constructions of BIBDs in section four. Meanwhile, we give a classification of the constructed BIBDs. The results are stated mainly in the following places: Theorem 2.7, Theorem 3.5, Corollary 3.6, Theorem 4.4, Theorem 4.9, Theorem 4.10, and Theorem 4.14 to Theorem 4.25. Since the construction is possible from a finite nearfield, we introduce this structure here. A *left nearfield* is an algebraic structure $(F, +, \cdot)$ such that $(F, +)$ is a group, $(F^* = F \setminus \{0\}, \cdot)$ is also a group, and $\cdot$ satisfies the left distributive law with respect to $+$: $a \cdot (b + c) = a \cdot b + a \cdot c$ for any a, b, and c in F. Similarly, we can also define a right nearfield. For more facts about nearfields, the reader is referred to Clay's or Wähling's books [12, 23].

2. Simple BIBDs From Finite Nearfields

In this section we will develop a method for constructing BIBDs. We also analyze the basic structures of the constructions.

Let us assume that $(F, +, \cdot)$ is a finite left nearfield (or just a finite field) with $|F| = q$ and characteristic $charF = p$. Let S be a proper subset of F and $|S| = k \geq 2$. We call S a *generating block*. For any nonempty subset B of F and any $b \in F^*$, $a \in F$, we use the following notations: $bB = \{bx \mid x \in B\}$ and $B - a = \{x - a \mid x \in B\}$. Define $\mathcal{B} = \{bS + a \mid b \in F^*, a \in F\}$.

The following tells that all blocks in $\mathcal{B}$ are of the same size. Besides, $\mathcal{B}$ is invariant under certain transformations.

Theorem 2.1. (1) *$|B| = |S|$ for any B in $\mathcal{B}$.*

(2) *$\mathcal{B}$ remains the same if S is replaced by $\beta S + \alpha$ or by $\beta(S + \alpha)$ for any $\beta \in F^*$ and any $\alpha \in F$.*

Define $\sim_c$ on F^* by $b_1 \sim_c b_2$ if there is $a \in F$ such that $b_1 S = b_2 S + a$. Then $\sim_c$ is an equivalence relation on F^*. Define $\sim_r$ on F by $a_1 \sim_r a_2$ if $S + a_1 = S + a_2$. Then $\sim_r$ is an equivalence relation on F. Let $n = |F^*/\sim_c|$ and let $\mu = |F/\sim_r|$. Let $T_c = \{b_1, b_2, \ldots, b_n\}$ be a set of representatives of the equivalence classes induced by $\sim_c$, and denote the equivalence class of b by $\overline{b}$. Also let $T_r = \{a_1, a_2, \ldots, a_\mu\}$ be a set of representatives of the equivalence classes induced by $\sim_r$, and denote the equivalence class of a by $\tilde{a}$.

We have some structures for the equivalence relation $\sim_c$ on F^* as follows.

Theorem 2.2. (1) *$\overline{1}$ is a subgroup of F^*.*

(2) *The equivalence classes induced by $\sim_c$ are exactly those left cosets of $\overline{1}$ in F^*; we have $\overline{b} = b\overline{1}$ for any $b \in F^*$.*

(3) *$F^* = \bigsqcup_{k=1}^{n} \overline{b_k} = \bigsqcup_{k=1}^{n} b_k \overline{1} = T_c \overline{1} = \bigsqcup_{\beta \in \overline{1}} T_c \beta$, where the symbol $\bigsqcup$ means disjoint union.*

(4) *$n = |F^*|/|\overline{1}|$.*

We also obtain some structures for the equivalence relation $\sim_r$ on F.

Theorem 2.3. (1) *$\tilde{0}$ is an additive subgroup of F.*

(2) *The equivalence classes induced by $\sim_r$ are exactly those cosets of $\tilde{0}$ in F; we have $\tilde{a} = a + \tilde{0}$ for any $a \in F$.*

(3) *$F = \bigsqcup_{k=1}^{\mu} \tilde{a_k} = \bigsqcup_{k=1}^{\mu} (a_k + \tilde{0}) = T_r + \tilde{0} = \bigsqcup_{\alpha \in \tilde{0}} (T_r + \alpha)$.*

(4) *$\mu = |F|/|\tilde{0}|$.*

(5) *S is a union of some cosets of $\tilde{0}$ and so $|\tilde{0}|$ divides $|S|$.*

(6) *If* $\sim_r$ *is nontrivial, that is,* $|\tilde{0}| > 1$, *then* $\gcd(|S|, |F|) > 1$.

Corollary 2.4. *For any nonempty proper subset* $S \subset F$ *with* $p \nmid |S|$, $\sim_r$ *is trivial and therefore* $\mu = q$.

Theorem 2.5. *If* S *is an additive subgroup of* F, *then* $\tilde{0} = S$.

We find all the distinct blocks in $\mathcal{B}$. Therefore, the size of $\mathcal{B}$ is determined.

Theorem 2.6. (1) $\mathcal{B} = \{b_i(S + a_j) \mid 1 \leq i \leq n,\ 1 \leq j \leq \mu\}$.
(2) $b = |\mathcal{B}| = \mu n$.

Proof. These can be asserted by showing (1) and (2) below.

(1) $bS + a = b_i(S + a_j)$ for some $b_i \in T_c$ and some $a_j \in T_r$.
(2) For any $b_{i_1}, b_{i_2} \in T_c$ and $a_{j_1}, a_{j_2} \in T_r$, $b_{i_1}(S + a_{j_1}) = b_{i_2}(S + a_{j_2})$ if and only if $i_1 = i_2$ and $j_1 = j_2$. ∎

The main result of this section is as follows.

Theorem 2.7. (1) $(F, \mathcal{B})$ *is a simple BIBD with parameters* $v = q$, $b = \mu n = |F/{\sim_r}| \cdot |F^*/{\sim_c}|$, $r = \frac{\mu n k}{q}$, $k = |S|$, *and* $\lambda = \frac{\mu n k(k-1)}{q(q-1)}$.
(2) $\{b_1 S, b_2 S, \ldots, b_n S\}$ *is a difference family if* $\sim_r$ *is trivial, and a partial difference family if* $\sim_r$ *is nontrivial.*
(3) *If* $p \neq 2$ *and* $|\overline{1}|$ *is odd, then the BIBD* $(F, \mathcal{B})$ *can be partitioned into two isomorphic simple BIBDs with parameters* $v = q$, $b = \frac{\mu n}{2}$, $r = \frac{\mu n k}{2q}$, $k = |S|$, *and* $\lambda = \frac{\mu n k(k-1)}{2q(q-1)}$.

Proof. Since $\mathcal{B} - c = \mathcal{B}$, the number of blocks in $\mathcal{B}$ containing c is the same as the number of blocks in $\mathcal{B}$ containing 0. Since $|S| \geq 2$, we have $\{0, 1\}$ is a subset of some block. One candidate is $(y - x)^{-1}(S - x) \in \mathcal{B}$ where $x, y \in S$ and $x \neq y$. It remains to show that every pair $\{c, d\}$, $c \neq d$, appears the same number of times as $\{0, 1\}$ does. This follows from the equation $(d - c)^{-1}(\mathcal{B} - c) = \mathcal{B}$. This proves (1). Part (2) is a consequence of (1). To prove (3), note that b_i and $-b_i$ are in different cosets of $\overline{1}$ for any i since $p \neq 2$ and $|\overline{1}|$ is odd. So $-b_i S = b_j S + a$ for some $j \neq i$ and some a. However, $b_i S$ and $-b_i S$ have the same difference lists. Thus these $b_i S$ can be put into two parts such that $b_i S$ and $b_j S = -b_i S - a$ are each in different parts (n is sure to be even). The difference lists of these two parts are the same. Therefore the statement follows since their union forms a (partial) difference family. The map $x \mapsto -x$ is an isomorphism of these two designs. ∎

2.1. Zero-Sum Generating Blocks

If $\sum_{x\in S} x = 0$, we say that S is a *zero-sum generating block* (abbreviated as ZSGB). When $p \nmid k$, we can assume S is a ZSGB, since if we let $s = \left(\sum_{x\in S} x\right) k^{-1}$ and $S' = S - s$, then the summation for S' is zero and S' generates the same $\mathcal{B}$ as S does. Moreover, we can assume $1 \in S$. This is because $\mathcal{B}$ remains the same if S is replaced by any βS for $\beta \in F^*$.

Definition 2.1.

(1) Let S be a zero-sum generating block. Then it is *of the first type* if $0 \notin S$. Otherwise, it is *of the second type*. A ZSGB containing 1 is abbreviated as ZSGBO.

(2) For any nonempty subset S of F, define S to be a generating block *of the first type* if there exist $\beta \in F^*$ and $\alpha \in F$ such that $\beta S + \alpha$ is a ZSGB of the first type; if there exist $\beta \in F^*$ and $\alpha \in F$ such that $\beta S + \alpha$ is a ZSGB of the second type, we say that S is *of the second type*.

(3) For any BIBD $(F, \mathcal{B})$ constructed in Theorem 2.7, we say $\mathcal{B}$ (or the BIBD) is *of the first type* if it is generated by a first-type block; $\mathcal{B}$ (or the BIBD) is *of the second type* if it is generated by a second-type block.

Theorem 2.8. *Suppose $p \nmid k$. Then any generating block $S \subset F$ with $|S| = k$ is either of the first type or of the second type. Therefore any BIBD with block size k is either of the first type or of the second type.*

For any generating block S, let $Stab_{F^*}(S) = \{b \in F^* \mid bS = S\}$, which is the stabilizer subgroup of S under the action of F^* on $\binom{F}{k}$.

In the following theorems, we investigate some properties of $Stab_{F^*}(S)$, especially when S is a zero-sum generating block.

Theorem 2.9.

(1) $Stab_{F^*}(S)S{=}S$; so $S\backslash\{0\}$ is a disjoint union of right cosets of $Stab_{F^*}(S)$.

(2) If $Stab_{F^*}(S)$ is nontrivial, then S is a ZSGB.

(3) $Stab_{F^*}(S) \subseteq S$ if S is a ZSGBO.

Theorem 2.10. *If S is a zero-sum generating block and $p \nmid k$, where $k = |S|$, then*

(1) $\beta_1 \sim_c \beta_2 \Longleftrightarrow \beta_1 S = \beta_2 S$*, and so* $\overline{1} = Stab_{F^*}(S)$*;*

(2) $|Stab_{F^*}(S)|$ *divides* k *if* S *is of the first type;*

(3) $|Stab_{F^*}(S)|$ *divides* $(k-1)$ *if* S *is of the second type;*

(4) $\{bS \mid b \in F^*\} = \{b_1 S, b_2 S, \ldots, b_n S\}$.

Note that when $p \nmid k$, we have $\sim_r$ is trivial by Corollary 2.4. Then $\mathcal{B} = \{b_i S + a \mid 1 \leq i \leq n,\ a \in F\}$. Therefore if F is a finite field with g a generator of F^*, we may choose $b_i = g^{(i-1)}$ for $1 \leq i \leq n$. That is, $\{S, gS, \ldots, g^{(n-1)}S\}$ is a difference family for $(F, \mathcal{B})$.

Example 2.1. If S is a nontrivial multiplicative subgroup of F^*, then S is a first-type ZSGBO; $\overline{1} = S$, and therefore $n = (q-1)/k$; $\sim_r$ is trivial, and hence $\mu = q$. So $(F, \mathcal{B})$ is a first-type simple BIBD with parameters $(q, k, k-1)$.

The following reveals certain connections between first-type ZSGBs and second-type ZSGBs.

Theorem 2.11.

(1) Suppose $S' = S \sqcup \{0\}$, then $Stab_{F^*}(S') = Stab_{F^*}(S)$.

(2) Suppose S is a first-type ZSGB and $p \nmid k(k+1)$; let $S' = S \sqcup \{0\}$. If the BIBD generated by S has parameters (q, k, λ), then the BIBD generated by S' has parameters $(q, k+1, \lambda(k+1)/(k-1))$. In particular, these two BIBDs have the same number of blocks.

(3) Suppose S is a second-type ZSGB and $p \nmid k(k-1)$; let $S'' = S \setminus \{0\}$. If the BIBD generated by S has parameters (q, k, λ), then the BIBD generated by S'' has parameters $(q, k-1, \lambda(k-2)/k)$. In particular, these two BIBDs have the same number of blocks.

2.2. The Possible Parameters

We now discuss the possible parameters of the BIBDs constructed in Theorem 2.7 when $p \nmid k$. Since $\tilde{0}$ is trivial and so $\mu = q$ at this time, it is enough to focus on the value $c = |\overline{1}|$. If $(F, \mathcal{B})$ is a first-type BIBD, then c divides k. We also know that c divides $q-1$. Therefore the parameters for a first-type BIBD must be of the form $(q, k, k(k-1)/c)$ for $c \mid \gcd(k, q-1)$. Similarly, we obtain that the parameters for a second-type BIBD must be of the form $(q, k, k(k-1)/c)$ for $c \mid \gcd(k-1, q-1)$.

We have developed a method for constructing BIBDs from generating blocks of finite nearfields. The basic structures of the constructions are analyzed.

3. The Constructions From Finite Fields

In this section we will show that, in a finite field, ZSGBOs with given stabilizers do exist except in some situations. Thereafter, various BIBDs with the possible parameters mentioned above can be obtained.

We assume that p is a prime and $q = p^{\alpha}$. Let $(F, +, \cdot)$ be the finite field with $|F| = q$ and let g be a generator of F^{*}. Recall that $Stab_{F^*}(S)$ is equal to $\overline{1}$ when $p \nmid k$ and S is a ZSGB with $|S| = k$. For $3 \leq k \leq q-4$, we are going to construct a first-type ZSGBO S such that $|S| = k$ and $|Stab_{F^*}(S)| = c$ where c is any number with $c \mid \gcd(k, q-1)$. The exceptions are when (1) $q = 7$, $k = 3$, and $c = 1$, or (2) $q = 9$, $k = 4$, and $c = 1$. For $4 \leq k \leq q-3$ and c is any number with $c \mid \gcd(k-1, q-1)$, we are going to construct a second-type ZSGBO S such that $|S| = k$ and $|Stab_{F^*}(S)| = c$. There are also exceptions when (1) $q = 7$, $k = 4$, and $c = 1$, or (2) $q = 9$, $k = 5$, and $c = 1$.

Therefore, for $3 \leq k \leq q-4$, we obtain a first-type BIBD with parameters $(q, k, k(k-1)/c)$ when $p \nmid k$ and c is any divisor of $\gcd(k, q-1)$. For $4 \leq k \leq q-3$, when $p \nmid k$ and c is any divisor of $\gcd(k-1, q-1)$, a second-type BIBD with the above parameters is also constructed. The corresponding exceptions are indicated as in the above paragraph. Moreover, if $p \neq 2$ and c is an odd number in these constructions, simple BIBDs with parameters $(q, k, k(k-1)/2c)$ can be obtained.

We are going to establish three lemmas, which will be applied in the proof of Theorem 3.5. The constructions in Lemma 3.3 and Lemma 3.4 rely mainly on the following theorem.

Theorem 3.1. *We assume that p is a prime, $q = p^{\alpha}$, $3 \leq k \leq q-3$, and $\gcd(k, q-1) > 1$. Let $(F, +, \cdot)$ be the finite field with $|F| = q$. Let c be any divisor of $\gcd(k, q-1)$ and let Φ be the subgroup of F^* with $|\Phi| = c$. Suppose that S is a first-type ZSGBO, $|S| = k$, and $\Phi S = S$. For any prime divisor u of $\gcd(k, q-1)/c$, define z_u according to*

(1) *if $u \nmid c$, then let $z_u = g^{(q-1)/u}$;*

(2) *if $u \mid c$ and suppose $u^w \parallel c$, then let $z_u = g^{(q-1)/y}$ where $y = u^{(w+1)}$.*

We have $Stab_{F^*}(S) = \Phi$ if for any prime divisor u of $\gcd(k, q-1)/c$, there is $x \in \langle z_u \rangle \setminus \Phi$ such that $x \notin S$. In particular, if $z_u \notin S$ for any prime divisor u of $\gcd(k, q-1)/c$, then we have $Stab_{F^*}(S) = \Phi$.

Proof. It is clear that Φ is a subgroup of $Stab_{F^*}(S)$. We also have that $|Stab_{F^*}(S)|$ divides $\gcd(k, q-1)$. So $Stab_{F^*}(S)$ is in the subgroup of order $\gcd(k, q-1)$. We consider the possibility that Φ is a proper subgroup of $Stab_{F^*}(S)$. Then S must contain some subgroup $\langle z_u \rangle$, where u is a prime divisor of $\gcd(k, q-1)/c$ and z_u is defined above. Thus if we exclude all the possible cases in choosing S, we get $Stab_{F^*}(S) = \Phi$. ∎

Lemma 3.2. *When $3 \leq k \leq (q-1)/2$ and $\gcd(k, q-1) = 1$, there is a first-type ZSGBO in F with $|S| = k$ such that $Stab_{F^*}(S)$ is trivial.*

Proof. Any first-type ZSGBO S with $|S| = k$ has trivial $Stab_{F^*}(S)$ since $|Stab_{F^*}(S)|$ divides $\gcd(k, q-1)$. We construct such a generating block S according to $p \neq 2$ or $p = 2$ in the following.

- The case for $p \neq 2$.

  Since $q-1$ is even, we have that k is an odd number. We then choose S as $S = (T \sqcup \{1, t-1\}) \setminus \{t\}$ where T satisfies: (1) $0, 1 \notin T$, (2) $x \in T \Leftrightarrow -x \in T$, and (3) $|T| = k-1$. The element $t \in T$ is any one with $t \neq 2$ and $t-1 \notin T$. There are $\binom{(q-3)/2}{(k-1)/2}$ choices of T that meets these three conditions. Any S specified above is a first-type ZSGBO with $|S| = k$. For example, when $\alpha = 1$ (so $F = Z_p$), our first choice of S is

  $$S = \left(T \sqcup \left\{1, \frac{p-k}{2}\right\}\right) \setminus \left\{\frac{p-k+2}{2}\right\}$$

  where

  $$\begin{aligned} T &= \left\{\frac{p}{2} \pm \frac{2i-1}{2} \mid i = 1, \ldots, \frac{k-1}{2}\right\} \\ &= \left\{\frac{p-k+2}{2}, \frac{p-k+4}{2}, \ldots, \frac{p+k-2}{2}\right\}. \end{aligned}$$

- The case for $p = 2$.

  (1) If $k = 4i$ for $i \geq 1$, we choose S as $S = t^{-1}T$ where T satisfies: (1) $0, 1 \notin T$, and (2) $2i$ disjoint pairs x, $x+1$ are in T. The element t is in T. There are $\binom{(q-2)/2}{2i}$ choices of such T that meets these three conditions. Any S specified above is a first-type ZSGBO with $|S| = k$.

  (2) If $k = 4i + 3$ for $i \geq 0$, we first construct a first-type ZSGBO S_1 with $|S_1| = 3$. We take F as an α-dimensional vector space over Z_2 for $\alpha \geq 3$. Let $\{e_1 = 1, e_2, \ldots, e_\alpha\}$ be a basis of F over Z_2. Then $S_1 = \{e_1, e_2, e_1 + e_2\}$ is a first-type ZSGBO. When $i \geq 1$, we then choose T so that (1) $e_1, e_2, e_1 + e_2 \notin T$, and (2) $2i$ disjoint pairs x, $x+1$ are in T. If $i = 0$, we let T be the empty set. There are $\binom{(q-4)/2}{2i}$ choices of such T. Next let $S = S_1 \sqcup T$. Then S is a first-type ZSGBO with $|S| = k$.

  (3) If $k = 4i + 5$ for $i \geq 0$, the proof is similar. We construct a first-type ZSGBO $S_1 = \{e_1 = 1, e_2, e_3, e_4, e_1+e_2+e_3+e_4\}$. There are $\binom{(q-10)/2}{2i}$ choices of T.

  (4) If $k = 4i + 6$ for $i \geq 0$, also by similar proof. We construct a first-type ZSGBO $S_1 = \{e_1 = 1, e_2, e_3, e_4, e_1+e_2, e_3+e_4\}$. There are $\binom{(q-10)/2}{2i}$ choices of T. ∎

Lemma 3.3. *When* $3 \leq k \leq (q-1)/2$, c *divides* $\gcd(k, q-1)$, *and* $c > 1$, *there is a first-type ZSGBO in* F *with* $|S| = k$ *such that* $|Stab_{F^*}(S)| = c$.

Proof. Suppose that $\gcd(k, q-1) = cd$, $q - 1 = cde$, and $k = cdh$. Let $\Phi = \left\langle g^{(q-1)/c} \right\rangle$, so $|\Phi| = c$. If $d = 1$, then $S = \bigsqcup_{i=1}^{h} \beta_i \Phi$ with $\beta_1 = 1$ (as a union of h distinct cosets of Φ) is a first-type ZSGBO such that $|S| = k$ and $Stab_{F^*}(S) = \Phi$. There are $\binom{(q-1)/c-1}{h-1}$ choices of such S.

So we suppose that $d > 1$ and let $d = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Define $z_1, z_2, \ldots, z_m$ as follows:

(1) if $p_j \nmid c$, then let $z_j = g^{(q-1)/p_j}$;

(2) if $p_j \mid c$ and suppose $p_j^w \parallel c$, then let $z_j = g^{(q-1)/y}$ where $y = p_j^{(w+1)}$.

We then choose $S = \bigsqcup_{i=1}^{dh} \beta_i \Phi$ where $\beta_1 = 1$ and $\beta_2, \ldots, \beta_{dh}$ are chosen such that $z_j \notin S$ for $1 \leq j \leq m$. Since $m \ll d$ and $e \geq 2h$, we have $d(e-h) \geq dh > m$. So $(q-1)/c - m = de - m > dh$. That means even $z_1, z_2, \ldots, z_m$ are exactly in m distinct cosets of Φ, we still have $\binom{(q-1)/c-m-1}{dh-1}$ many choices for S. It is clear that $|S| = k$, S is a first-type ZSGBO, and $\Phi S = S$. Also S satisfies the rest requirements in Theorem 3.1. Hence $Stab_{F^*}(S) = \Phi$. ■

Lemma 3.4. *When* $3 \leq k \leq (q-1)/2$ *and* $\gcd(k, q-1) > 1$, *there is a first-type ZSGBO in* F *with* $|S| = k$ *such that* $Stab_{F^*}(S)$ *is trivial, except for* $(q, k) = (7, 3)$ *or* $(9, 4)$.

Proof. We discuss this part in two situations: $q - 1 > 2k$ and $q - 1 = 2k$. Therefore $p \neq 2$ in the second situation.

- The case for $q - 1 > 2k$.

  We choose a larger prime divisor c' of $\gcd(k, q-1)$. Suppose $\gcd(k, q-1) = c'd$, $q - 1 = c'de$, $k = c'dh$, and $d = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Let $g_1 = g^{(q-1)/c'}$ and let $\Phi = \langle g_1 \rangle$. We first construct a set T, as in Lemma 3.3, for $c = c'$, so that T is a first-type ZSGBO with $|T| = k$ and $Stab_{F^*}(T) = \Phi$, where $|\Phi| = c'$. If $d \neq 1$, let $z_1, z_2, \ldots, z_m$ be defined as in the proof of Lemma 3.3. Let $M = \{0, z_1, z_2, \ldots, z_m\}$ if $d \neq 1$; let $m = 0$ and $M = \{0\}$ if $d = 1$. We then choose $z \in T \setminus \{1, g_1\}$. Consider the following two sets:

$$A = \{x \mid g_1 + x \notin T \sqcup M\}$$

  and

$$B = \{x \mid z - x \notin T \sqcup M\}.$$

  Each set has $q - 1 - k - m$ elements. Note that $0 \notin A \cup B$. So we have $|A \cap B| = |A| + |B| - |A \cup B| \geq q - 1 - 2k - 2m = c'd(e - 2h) - 2m \geq$

$c'd - 2m \geq 2$. Therefore there is an x_0 such that $g_1 + x_0, z - x_0 \notin T \sqcup M$, $g_1 + x_0 \neq z - x_0$, and $g_1 + x_0 \neq z$. Let $S = (T \sqcup \{g_1 + x_0, z - x_0\}) \setminus \{g_1, z\}$. Then we have that $Stab_{F^*}(S)$ is trivial by Theorem 3.1. Clearly, S is a first-type ZSGBO with $|S| = k$.

- The case for $k = (q-1)/2$.

  We have $q = 2k+1 = p^\alpha$. Let $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ with $p_1 < p_2 < \cdots < p_m$ and let $\Phi_i = \left\langle g^{(q-1)/p_i} \right\rangle$ for $1 \leq i \leq m$. Here the discussions are arranged according to different values of q and p, in order for technical details.

  (1) If $q = 4h+1$ and $p \geq 5$, then $k = 2h$ and $p_1 = 2$. In order to apply Theorem 3.1, we need to choose a subset T such that (1) $x \in T \Leftrightarrow -x \in T$, (2) $\pm 1 \in T$ and $0, \pm 2 \notin T$, (3) $|(T \cap \Phi_i) \setminus \{1\}| \geq 2$ for any $i \neq 1$, and (4) $|T| = k = 2h$. Moreover, we require that (5) there is $x_0 \in T \setminus \{\pm 1, 3\}$ such that $x_0 - 1 \notin T$.

  When can we have this choice of T? We claim that the choice is always possible as long as $k \geq 4m$. There are exactly h pairs $\{x, -x\}$ in T. To fulfill condition (3) we need at most $2(m-1)$ pairs. The problem is mainly on the suitable choice of x_0.

  In the beginning we put ± 1 in T. Next we put at most $2(m-1)$ pairs in T as in condition (3). If there is no such x_0 mentioned in condition (5) for the current T, then we choose a such x_0 and put $\pm x_0$ in T. If the current $|T|$ is less than k, we continue choosing other pair not in $T \sqcup \{0, \pm 2, \pm(x_0 - 1)\}$ and putting this pair in T until T has h pairs. Thus when $h - 2 \geq 2(m-1)$ this can always be done; that is, when $k \geq 4m$. Let $T' = (T \sqcup \{2, x_0 - 1\}) \setminus \{1, x_0\}$ and let $S = F^* \setminus T'$. Then S is a first-type ZSGBO such that $|S| = k$ and $Stab_{F^*}(S)$ is trivial by Theorem 3.1. Note that $|T' \cap \Phi_i| \geq 1$ for any i.

  When is $k < 4m$? It is certainly impossible if $m \geq 3$. So $(m, k) = (1, 3)$ or $(2, 6)$. We only consider even k here. For $q = 13$ and $k = 6$, the set $S = \{1, 2, 3, 4, 5, 11\}$ is a first-type ZSGBO with trivial $Stab_{F^*}(S)$. For another construction, we can use the method as in the last paragraph. Note that $\Phi_2 = \{1, 3, 9\}$. So we let $T = \{1, 3, 4 = -9, 9, 10 = -3, 12 = -1\}$, $x_0 = 9$, and $T' = \{2, 3, 4, 8, 10, 12\}$. Therefore $S = \{1, 5, 6, 7, 9, 11\}$ meets the requirements.

  (2) When $q = 4h+1 = 3^\alpha = 9^\beta$ for $\beta \geq 2$, then $h \geq 20$. We are going to choose T so that (1) $0, 1, 2 \notin T$, (2) $x \in T \Leftrightarrow -x \in T$, (3) $|T \cap \Phi_i| \geq 2$ for any $i \neq 1$, and (4) $|T| = k = 2h$. Moreover, we require that (5) there exist $x_1, x_2 \in T$ such that (i) $x_1 \neq \pm x_2$, (ii) $\{x_1, x_2\} \nsubseteq \Phi_i$ for any i, (iii) $x_1 + 1, x_2 - 1 \notin T$, and (iv) $x_1 + 1 \neq x_2 - 1$. How to have this choice of T? First we choose x_1, x_2 in (5), then there are at least

$(q-3-4-4)/2$ distinct pairs $\{\pm x\}$ left for chosen in order to fulfill conditions (3) and (4). And we still need $h-2$ pairs. Since $k \geq 4m$ (so $h-2 \geq 2(m-1)$) and $(q-11)/2 > h-2$, we conclude that this choice of T is always possible. Let $T' = (T \sqcup \{x_1+1, x_2-1\}) \setminus \{x_1, x_2\}$ and let $S = F^* \setminus T'$. Then S is a first-type ZSGBO such that $|S| = k$. Note that $x_1, x_2 \in S$ and $-x_1, -x_2 \notin S$; so $-1 \notin Stab_{F^*}(S)$. Also $|T' \cap \Phi_i| \geq 1$ for any $i \neq 1$; so $\Phi_i \nsubseteq Stab_{F^*}(S)$ for any $i \neq 1$. Therefore $Stab_{F^*}(S)$ is trivial.

(3) For $q = 9$ and $k = 4$, there is no first-type ZSGBO S with trivial $Stab_{F^*}(S)$; while there exists second-type ZSGBO with trivial $Stab_{F^*}(S)$. Let $F = GF(9) \cong Z_3[x]/(x^2+1)$ and suppose $u \in F$ is a root of $x^2+1=0$. We have that $S = \{0, 1, u, 2u+2\}$ is a second-type ZSGBO with trivial $Stab_{F^*}(S)$. Therefore S generates a $(9, 4, 12)$ BIBD. To show that there is no first-type ZSGBO S with trivial $Stab_{F^*}(S)$. Suppose $S = \{1, x_1, x_2, x_3\}$ is such a set. Then $x_1, x_2, x_3 \in \{\pm u, \pm(u+1), \pm(u+2)\}$ are all distinct, and the sum of any two of them is not zero– otherwise we will have $S = -S$. Consider the pair $\{x_1, x_2\}$ first. We have twelve (i.e., $6 \cdot 4/2$) choices of this pair. However, for any of these choices, there is no solution of x_3 such that S is a first-type ZSGBO.

(4) If $q = 4h+3$ and $p \geq 11$, then $k = 2h+1$. We are going to choose T such that (1) $2, 3, -5 \in T$ and $0, \pm 1, -2, -3, 5 \notin T$, (2) $x \in T \setminus \{2, 3, -5\} \Rightarrow -x \in T$, (3) $|T \cap \Phi_i| \geq 1$ for any i, and (4) $|T| = k = 2h+1$. Since $k \geq 2m+3$ (so $h-1 \geq m$), we always have this choice of T. We first choose those m elements in (3), then at least we have $\binom{2h-3-m}{h-1-m}$ choices of T. Let $S = F^* \setminus T$. Then S is a first-type ZSGBO with trivial $Stab_{F^*}(S)$ by Theorem 3.1.

(5) When $q = 4h+3 = 7^\alpha = 7^{2\beta+1}$ for $\beta \geq 1$, then $h \geq 85$. We are going to choose T such that (1) $1, 2, 4 \in T$ and $0, 3, 5, 6 \notin T$, (2) $x \in T \setminus Z_7 \Rightarrow -x \in T$, (3) $|(T \cap \Phi_i) \setminus \{1\}| \geq 2$ for any i, and (4) $|T| = k = 2h+1$. Moreover, we require that (5) there exists $x_0 \in T \setminus \{1, 2\}$ so that $x_0 - 2 \notin T$. We first choose x_0 in (5) and those $2m$ elements in (3), then at least we have $\binom{2h-4-2m}{h-2-2m}$ choices of T. Note that $2h+1 = k \geq 4m+5$. Let $T' = (T \sqcup \{3, x_0-2\}) \setminus \{1, x_0\}$ and let $S = F^* \setminus T'$. Then S is a first-type ZSGBO such that $|S| = k$ and $Stab_{F^*}(S)$ is trivial by Theorem 3.1.

(6) When $q = 4h+3 = 3^\alpha = 3^{2\beta+1}$ for $\beta \geq 1$, then $h \geq 6$. We are going to choose T so that (1) $1, 2 \in T$ and $0 \notin T$, (2) $x \in T \Leftrightarrow -x \in T$, (3) $|(T \cap \Phi_i) \setminus \{1\}| \geq 2$ for any i, and (4) $|T| = 2h+2$. Moreover, we require that (5) there exists $x_0 \in F^* \setminus T$ so that $x_0 - 1 \in T$. We first choose x_0 in (5) and those $2m$ elements in (3), then at least we

have $\binom{2h-2-2m}{h-1-2m}$ choices of T. Note that $2h+1=k\geq 4m+3$. Let $T'=F^*\setminus T$ and let $S=(T'\sqcup\{1,x_0-1\})\setminus\{x_0\}$. Then S is a first-type ZSGBO such that $|S|=k$ and $Stab_{F^*}(S)$ is trivial by Theorem 3.1.

(7) For $q=7$ and $k=3$, a first-type ZSGBO with trivial $Stab_{F^*}(S)$ is impossible. It is because that we have at most 35 distinct blocks here, while such a ZSGBO will generate a BIBD with 42 blocks. ∎

Now we introduce the main result of this section.

Theorem 3.5. *We assume that p is a prime and $q=p^\alpha$. Let $(F,+,\cdot)$ be the finite field with $|F|=q$. For $3\leq k\leq q-4$, there is a first-type ZSGBO S such that $|S|=k$ and $|Stab_{F^*}(S)|=c$ where c is any divisor of $\gcd(k,q-1)$. The exceptions are when $(q,k,c)=(7,3,1)$ or $(9,4,1)$. For $4\leq k\leq q-3$ and c is any divisor of $\gcd(k-1,q-1)$, there is a second-type ZSGBO S such that $|S|=k$ and $|Stab_{F^*}(S)|=c$. There are also exceptions when $(q,k,c)=(7,4,1)$ or $(9,5,1)$.*

Proof.

(1) As a result of the above three lemmas, we have for $3\leq k\leq (q-1)/2$, there is a first-type ZSGBO S such that $|S|=k$ and $|Stab_{F^*}(S)|=c$ where c is any number with $c\mid\gcd(k,q-1)$. The exceptions are when $(q,k,c)=(7,3,1)$ or $(9,4,1)$.

(2) When $4\leq k\leq (q+1)/2$ and c is any divisor of $\gcd(k-1,q-1)$, suppose S_1 is a first-type ZSGBO such that $|S_1|=k-1$ and $|Stab_{F^*}(S_1)|=c$. Let $S=S_1\sqcup\{0\}$, then S is a second-type ZSGBO such that $|S|=k$ and $|Stab_{F^*}(S)|=c$. The exceptions are when $(q,k,c)=(7,4,1)$ or $(9,5,1)$.

(3) When $(q-1)/2\leq k\leq q-4$ and c is any divisor of $\gcd(k,q-1)$, suppose S_2 is a second-type ZSGBO such that $|S_2|=q-k$ and $|Stab_{F^*}(S_2)|=c$. Note that $\gcd(q-k-1,q-1)=\gcd(k,q-1)$. We next choose $s\in F\setminus S_2$ and let $S=s^{-1}(F\setminus S_2)$. Then S is a first-type ZSGBO such that $|S|=k$ and $|Stab_{F^*}(S)|=c$. The exceptions are when $(q,k,c)=(7,3,1)$ or $(9,4,1)$.

(4) When $(q+1)/2\leq k\leq q-3$ and c is any divisor of $\gcd(k-1,q-1)$, suppose S_3 is a first-type ZSGBO such that $|S_3|=k-1$ and $|Stab_{F^*}(S_3)|=c$. Let $S=S_3\sqcup\{0\}$, then S is a second-type ZSGBO such that $|S|=k$ and $|Stab_{F^*}(S)|=c$. The exceptions are when $(q,k,c)=(7,4,1)$ or $(9,5,1)$. ∎

Corollary 3.6. *Let p be a prime and let $(F,+,\cdot)$ be the finite field with $|F|=q=p^\alpha$. For $3\leq k\leq q-4$, there is a first-type BIBD with parameters $(q,k,k(k-1)/c)$ when $p\nmid k$ and c is any divisor of $\gcd(k,q-1)$. The exceptions are when $(q,k,c)=(7,3,1)$ or $(9,4,1)$. For $4\leq k\leq q-3$, when $p\nmid k$ and c is any divisor of $\gcd(k-1,q-1)$, a second-type BIBD with the above parameters also exists.*

The exceptions are when $(q, k, c) = (7, 4, 1)$ *or* $(9, 5, 1)$. *Moreover, if* $p \neq 2$ *and* c *is an odd number in these constructions, the BIBD can be partitioned into two isomorphic simple BIBDs with parameters* $(q, k, k(k-1)/2c)$.

Therefore, various BIBDs with the possible parameters mentioned in the end of section two can be obtained.

4. The Cases When $charF$ Divides the Block Size

In this section we focus on the remaining cases not considered in the last section. The situation becomes more complicated when the characteristic of the finite field divides the block size, as the reader is going to see.

Throughout this section, we assume that $(F, +, \cdot)$ is the finite field with $|F| = q = p^{\alpha}$, S is a proper subset of F, and p divides k, where $k = |S|$. For a generating block S with $p \mid k$, it may happen that $bS + a$ is never a ZSGB for any $b \in F^*$ and any $a \in F$. For example, let $F = GF(9)$ and let u be a root of $x^2 + 1 = 0$. Then $S = \{1, 2, u\}$ is such a block. These kinds of blocks always generate $(q, k, k(k-1))$ BIBDs when $p \neq 2$.

Theorem 4.1. *If* p *divides* k, *where* $k = |S|$, *and* S *is not a ZSGB, then* $\overline{1}$ *is trivial and so is* $Stab_{F^*}(S)$.

Theorem 4.2. *Any additive subgroup* H *of* F *with* $|H| \neq 2$ *has zero sum.*

Proof. When $p \neq 2$, this can be seen easily since we can put all nonzero elements of H into distinct pairs $\{\pm x\}$. When $p = 2$, we consider that any additive subgroup is also a vector space over Z_p. Let $\{e_1, e_2, \ldots, e_m\}$ be a basis of H over Z_2, where m is the dimension of H. For any i with $1 \leq i \leq m$, consider the number of occurrences of e_i in the representation of all nonzero elements in H. It is 2^{m-1}, which is even since $m \geq 2$. Therefore H has zero sum. Hence the statement follows. ∎

Theorem 4.3. *Suppose* $S \subset F$ *and* $|\tilde{0}| \neq 1, 2$, *then* S *is a ZSGB.*

Proof. Consider $S = S + \tilde{0} = \sqcup_{i=1}^{\ell}(a_i + \tilde{0})$ as a disjoint union of additive cosets of $\tilde{0}$, so $k = \ell|\tilde{0}|$. Since $\tilde{0}$ is not trivial, we get p divides $|\tilde{0}|$. Therefore

$$\sum_{x \in S} x = \sum_{i=1}^{\ell} \left(\sum_{x \in a_i + \tilde{0}} x \right) = \sum_{i=1}^{\ell} |\tilde{0}| a_i = 0.$$

Note that $\sum_{x\in\tilde{0}} x = 0$ if $|\tilde{0}| \neq 2$. Hence S is a ZSGB. ■

When $|\tilde{0}| = 2$ (so $p = 2$), S is a ZSGB if and only if 4 divides k. It is because the sum of any coset of $\tilde{0}$ is 1. The interesting fact is that Z_2 is the only finite field which does not have the zero-sum property.

The following theorem is a consequence of the above theorems.

Theorem 4.4. *For any k with $3 \leq k \leq q-3$ and $p \mid k$, when $p \neq 2$ or $k \equiv 2 \pmod 4$, there is always a $(q, k, k(k-1))$ simple BIBD; there is also a $(q, k, k(k-1)/2)$ simple BIBD.*

Proof. It is easy to find a set $S \subset F$ such that $|S| = k$ and S is not a ZSGB. When $p = 2$ and $k \equiv 2 \pmod 4$, S can be chosen so that $|\tilde{0}| = 1$ or $|\tilde{0}| = 2$. When $p \neq 2$, a $(q, k, k(k-1)/2)$ BIBD is obtained by Theorem 2.7 (3). ■

When $p \nmid k$, we know that a generating block is either of the first-type or of the second-type. What happens when $p \mid k$ for a ZSGB? If S is a first-type ZSGB, choose $s \in S$. Then $S - s$ is a second-type ZSGB; so S is a generating block of the second-type. Conversely, if S is a second-type ZSGB, choose $s \notin S$. Then $S - s$ is a first-type ZSGB; so S is a generating block of the first-type. Therefore, we need further properties for classifying ZSGBs.

Theorem 4.5. *Suppose S generates the BIBD $(F, \mathcal{B})$. Then there is an $a' \in F$ such that the translation $S' = S + a'$ satisfies $\overline{1}S' = S'$; i.e., $\overline{1} = Stab_{F^*}(S')$. At this time the collection $\{bS' \mid b \in F^*\}$ forms a difference family for $(F, \mathcal{B})$ if $\tilde{0}$ is trivial, or partial difference family for $(F, \mathcal{B})$ if $\tilde{0}$ is nontrivial.*

Proof. We have already known this result when $p \nmid k$. When $p \mid k$, it is clear if $\overline{1}$ is trivial. So we assume that $p \mid k$ and $\overline{1} = \langle b \rangle$ for $1 \neq b \in F^*$. Therefore we have $S = bS + a$ for some $a \in F$. Let $a' = a/(b-1)$, then we get $b(S + a') = S + a'$. Let $S' = S + a'$. It is clear that S and S' have the same $\overline{1}$ and S' also generates $(F, \mathcal{B})$. Since $\overline{1}S' = S'$, the statement follows. ■

Theorem 4.6.

(1) If $Stab_{F^*}(S)$ is nontrivial, then $\overline{1} = Stab_{F^*}(S)$.

(2) If $Stab_{F^*}(S)$ and $Stab_{F^*}(S + a)$ both are nontrivial, then $S = S + a$.

(3) Among all the distinct translations of a generating block, there is at most one with nontrivial stabilizer. When $\overline{1}$ is nontrivial, there is exact one such translation; all other translations have trivial stabilizers.

Proof.

(1) For any $b_2 \in \overline{1}$, we want to show that $b_2 \in Stab_{F^*}(S)$. First we choose $1 \neq b_1 \in Stab_{F^*}(S)$. Let $c = o(b_1)$. Then $S = b_1 S = b_2 S + a$ for some $a \in F$. We have $S = b_1^i S = b_1^i(b_2 S + a) = b_2(b_1^i S) + b_1^i a = b_2 S + b_1^i a$. Therefore $b_2 S = b_2 S + (b_1^i - 1)a$. By using this formula repeatedly, we get $b_2 S = b_2 S + (b_1^{c-1} - 1)a + (b_1^{c-2} - 1)a + \cdots + (b_1 - 1)a = b_2 S + (b_1^{c-1} + b_1^{c-2} + \cdots + b_1 + 1 - c)a = b_2 S - ca = b_2 S - jca = b_2 S + a = S$ where j is such that $-jc \equiv 1 \pmod{p}$. Since $\gcd(c, p) = 1$, there exists such j. Also note that $b_1^{c-1} + b_1^{c-2} + \cdots + b_1 + 1 = 0$. Hence $b_2 \in Stab_{F^*}(S)$ and we conclude that $\overline{1} = Stab_{F^*}(S)$.

(2) From the first result we have $\overline{1} = Stab_{F^*}(S) = Stab_{F^*}(S + a)$. We choose $1 \neq b \in \overline{1}$. Let $c = o(b)$. Then $S = b^i S$ and $S + a = b^i(S + a) = b^i S + b^i a = S + b^i a$ for any i. Therefore $S = S + (b^i - 1)a$ for any i. By using this formula repeatedly, we get $S = S + (b^{c-1} - 1)a + (b^{c-2} - 1)a + \cdots + (b - 1)a = S + (b^{c-1} + b^{c-2} + \cdots + b + 1 - c)a = S - ca = S - jca = S + a$ where j is such that $-jc \equiv 1 \pmod{p}$.

(3) This is a consequence of the above results. ■

Definition 4.2. Suppose S generates $(F, \mathcal{B})$ and p divides $k = |S|$.

(1) If S is not a ZSGB, we say that S is *of the fourth type*. If S is a ZSGB and $\overline{1}$ is trivial, we say that S is *of the third type*. When S is a ZSGB and $\overline{1}$ is not trivial, suppose $S = bS + a$ for $1 \neq b \in F^*$ and $a \in F$, we say that S is *of the refined first type* if $a/(1 - b) \notin S$; if $a/(1 - b) \in S$, we say that S is *of the refined second type*.

(2) We say that $\mathcal{B}$ (or the BIBD) is *of the refined first type*, *of the refined second type*, *of the third type*, or *of the fourth type* according to which type S is in the previous definition.

Are the definitions for refined types well defined? If S is a ZSGB with nontrivial $\overline{1}$ and $S = b_1 S + a_1 = b_2 S + a_2$ for $b_1, b_2 \in F^* \setminus \{1\}$, $a_1, a_2 \in F$. Then $S + a_1/(b_1 - 1) = S + a_2/(b_2 - 1)$ by Theorem 4.5 and Theorem 4.6(2). So we have $a_1/(1 - b_1) \in S$ if and only if $a_2/(1 - b_2) \in S$.

Theorem 4.7. *Suppose $Stab_{F^*}(S)$ is nontrivial. Then*

(1) $0 \notin S$ *if and only if* S *is of the refined first type;*

(2) $|Stab_{F^*}(S)|$ *divides* k *if and only if* S *is of the refined first type;*

(3) $|Stab_{F^*}(S)|$ *divides* $(k - 1)$ *if and only of* S *is of the refined second type.*

Corollary 4.8. *If S is a refined-type ZSGB, then*

(1) $|\overline{1}|$ *divides* k *if and only if* S *is of the refined first type;*

(2) $|\overline{1}|$ *divides* $(k-1)$ *if and only of* S *is of the refined second type.*

Theorem 4.9. *Any BIBD (or generating block) belongs to exactly one type.*

Proof. Firstly, S is not a ZSGB if and only if $bS+a$ is not a ZSGB for any $b \in F^*$ and any $a \in F$. So fourth-type BIBDs can only be generated by fourth-type generating blocks. Secondly, S and $bS+a$ have the same $\overline{1}$. So third-type BIBDs can only be generated by third-type generating blocks. Finally, if two ZSGBs S_1 and S_2 generate the same BIBD with nontrivial $\overline{1}$, by the previous corollary we know that S_1 and S_2 have the same refined type, since either $|\overline{1}|$ divides k or $|\overline{1}|$ divides $k-1$. We conclude that refined first-type (or second-type) BIBDs can only be generated by refined first-type (or second-type, resp.) generating blocks. ∎

At present, the following question is not fully resolved: is there a third-type ZSGBO? If it is true, how to find a such one?

On the other hand, for refined-type ZSGBOs, the answer is affirmative. By the process in the proof of Lemma 3.3, we can construct these kinds of generating blocks (the results are stated in Theorem 3.5). However, when can we have a construction with trivial $\sim_r$ (or $\tilde{0}$)?

Theorem 4.10. *Suppose* p *divides* k*. When* $c \neq 1$ *and* c *divides* $\gcd(k, q-1)$*, there is a refined first-type ZSGBO* S *such that* $|\overline{1}| = |Stab_{F^*}(S)| = c$*; when* $c \neq 1$ *and* c *divides* $\gcd(k-1, q-1)$*, there is a refined second-type ZSGBO* S *such that* $|\overline{1}| = |Stab_{F^*}(S)| = c$*. If any such* S *is with trivial* $\sim_r$*, then we have a* $(q, k, k(k-1)/c)$ *simple BIBD. In this case, if* $p \neq 2$ *and* c *is odd, we also have a* $(q, k, k(k-1)/2c)$ *simple BIBD by Theorem 2.7(3).*

In the rest part of this section, we give some constructions with nontrivial $\sim_r$ (or $\tilde{0}$). It is not difficult to get the following result.

Theorem 4.11. *The stabilizer* $Stab_{F^*}(S)$ *is a subgroup of* $Stab_{F^*}(\tilde{0})$*. Besides,* $\overline{1}$ *is a subgroup of* $Stab_{F^*}(\tilde{0})$*.*

Since $\tilde{0}$ is an additive subgroup, a study on the stabilizers of additive subgroups is needed.

Theorem 4.12. *If* S *is an additive subgroup of* F*, then* $Stab_{F^*}(S) = E^*$ *where* E *is the largest (in size) subfield of* F *such that* S *is a vector space over* E*.* E *is also the vector space over* Z_p *spanned by* $Stab_{F^*}(S)$*.*

Proof. Note that the vector space T over Z_p spanned by $Stab_{F^*}(S)$ is indeed a subfield of F. Then it is clear $Stab_{F^*}(S) \le T^*$. We also have S is a vector space over T. Therefore $T^* \le Stab_{F^*}(S)$ and so $Stab_{F^*}(S) = T^*$. If E is the largest subfield of F such that S is a vector space over E, then we have $E^* \le Stab_{F^*}(S) = T^*$. Since $|E| \ge |T|$, we get $E^* = Stab_{F^*}(S)$ and $E = T$. ■

Lemma 4.13. *If S is a nontrivial additive subgroup, let $c = |Stab_{F^*}(S)|$ and let $k = |S|$, then the BIBD generated by S has parameters $(q, k, (k-1)/c)$.*

Proof. We have known that $\tilde{0} = S$ from Theorem 2.5. Suppose $b \in \overline{1}$, then there is $a \in F$ such that $bS = S + a$. Since $b \cdot 0 = s + a$ for some $s \in S$, we get $a = -s \in S$. Therefore $bS = S$ and $b \in Stab_{F^*}(S)$. That is, $\overline{1} = Stab_{F^*}(S)$. Hence S generates a simple BIBD with parameters $(q, k, (k-1)/c)$. ■

Theorem 4.14. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d be any number such that $d < \alpha/\beta$. Then there is a refined second-type BIBD with parameters $(p^{\alpha}, p^{\beta d}, (p^{\beta d}-1)/(p^{\beta}-1))$. The design attains λ_{min} when $\gcd(d, \alpha/\beta) = 1$.*

Proof. Let E be the subfield of F with $|E| = p^{\beta}$. Let $S \subset F$ be a vector space over E such that $|S| = p^{\beta d}$ and S is not a vector space over any other larger subfield. Then we have $\tilde{0} = S$ and $Stab_{F^*}(S) = E^*$. How to choose the above S? Let $E_1 = Stab_{F^*}(S) \cup \{0\}$, then S is a vector space over E_1 and $E \subseteq E_1$. If E_1 contains E properly, then there is a subfield $E_u \subseteq E_1$ so that $E \subset E_u$ and the degree of E_u over E is a prime u. Let $h = \alpha/\beta$. We have u divides h, and u divides d if S is also a vector space over E_u. For each prime divisor u of $\gcd(h, d)$ we choose a vector in $E_u \setminus E$. So there are exactly ℓ vectors, say $v_1, v_2, \ldots, v_\ell$, where ℓ is the number of distinct prime divisors of $\gcd(h, d)$. We next extend $\{v_1, v_2, \ldots, v_\ell\}$ to be a basis $\{v_1, v_2, \ldots, v_\ell, v_{\ell+1} = 1, v_{\ell+2}, \ldots, v_{\ell+m}\}$ of F over E. Since $\ell + m = h$ and $\ell < h - d$ (by $\gcd(h, d) \le h - d$), we have $d < m$. Thus we can let S be the vector space over E spanned by $v_{\ell+1} = 1$ and any $d - 1$ vectors chosen from $\{v_{\ell+2}, \ldots, v_h\}$. Then S does not contain E_u for any prime divisor u of $\gcd(h, d)$. Therefore S does not contain any subfield larger than E. Hence S generates a refined second-type BIBD with parameters $v = p^{\alpha}$, $k = p^{\beta d}$, and $\lambda = (p^{\beta d}-1)/(p^{\beta}-1)$. Finally, notice that $\lambda_{min} = (p^{\beta d}-1)/(p^{\gcd(\beta d, \alpha)}-1)$. Therefore λ_{min} is attained when $\gcd(d, \alpha/\beta) = 1$. ■

With $h = \alpha/\beta$, two special cases of this construction are $AG_{h-1}(h, p^{\beta})$ (when $d = h - 1$) and $AG_1(h, p^{\beta})$ (when $d = 1$), where $AG_d(n, q')$ is the collection of all d-dimensional flats in the affine space $AG(n, q')$ [5, II.8.9].

We point out that the above construction is a resolvable BIBD. A *parallel class* in a design is a set of blocks which partition the point set. A *resolvable BIBD* (RBIBD) is a BIBD whose blocks can be partitioned into parallel classes. An *affine design* is a RBIBD such that any two blocks from distinct parallel classes intersect in a constant number of points. It is known that for a RBIBD with parameters (v, b, r, k, λ), the design is also an affine design if and only if $b = v+r-1$ (or equivalently, $r = k+\lambda$). In this case, any two blocks from distinct parallel classes have exactly k^2/v points in common.

Theorem 4.15. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d be any number such that $d < \alpha/\beta$. Then there is a $(p^{\alpha}, p^{\beta d}, (p^{\beta d}-1)/(p^{\beta}-1))$ RBIBD. There is also a $(p^{\alpha}, p^{\alpha-\beta}, (p^{\alpha-\beta}-1)/(p^{\beta}-1))$ affine design, in which any two blocks from distinct parallel classes intersect in $p^{\alpha-2\beta}$ points.*

Proof. Note that all the additive cosets $S + a_j$, $1 \leq j \leq \mu$, of S form a parallel class. Recall that $\mathcal{B} = \{b_i(S + a_j) \mid 1 \leq i \leq n,\ 1 \leq j \leq \mu\}$, as indicated in Theorem 2.6. It is then clear that $\mathcal{B}$ is partitioned into parallel classes. So $(F, \mathcal{B})$ is a RBIBD. When $d = \alpha/\beta - 1$, we get $r = k + \lambda$, hence $(F, \mathcal{B})$ is an affine design in this case. ∎

For example, let $p = 2$, $\alpha = 6$, and $\beta = d = 2$ in the construction, then there exists a $(64, 16, 5)$ RBIBD, which is also an affine design. Let $p = 2$, $\alpha = 10$, and $\beta = d = 2$ in the construction, then there exists a $(1024, 16, 5)$ RBIBD. These two BIBDs attain their corresponding λ_{min}.

Theorem 4.16. *Let E be a subfield of F with $|E| = p^{\beta} > 2$. Let d and m be any number such that $d + m \leq \alpha/\beta$. Suppose there are c_i, $1 \leq i \leq m$, such that c_i divides $p^{\beta} - 1$ and $\gcd(c_1, c_2, \ldots, c_m) = c \neq 1$. Let Φ_i, $1 \leq i \leq m$, be the subgroups of E^* with $|\Phi_i| = c_i$.*

Let $S_0 \subset F$ be a d-dimensional vector space over E such that $|S_0| = p^{\beta d}$, $E \subseteq S_0$, and $Stab_{F^*}(S_0) = E^*$, as constructed in the proof of Theorem 4.14. Let $\{e_{m+1} = 1, e_{m+2}, \ldots, e_{m+d}\}$ be a basis of S_0 over E. Choose $e_i \in F$, $1 \leq i \leq m$, such that $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+d}$ are linearly independent over E.

Suppose that there are $S_i \subseteq E$, $1 \leq i \leq m$, such that (1) $Stab_{F^*}(S_i) = \Phi_i$ ($1 \leq i \leq m$), and (2) $S_i \neq S_i + x$ for any $x \neq 0$ ($1 \leq i \leq m$). Let $|S_i| = k_i$ for $1 \leq i \leq m$. Let $S = S_1e_1 + S_2e_2 + \cdots + S_me_m + S_0$. Then S generates a simple BIBD with parameters $v = p^{\alpha}$, $b = p^{\alpha-\beta d}(p^{\alpha}-1)/c$, $r = k_1k_2\cdots k_m(p^{\alpha}-1)/c$, $k = k_1k_2\cdots k_m p^{\beta d}$, and $\lambda = k_1k_2\cdots k_m(k_1k_2\cdots k_m p^{\beta d}-1)/c$. The BIBD is of the refined second type if $0 \in S_i$ for every i; otherwise, it is of the refined first type. If $p \neq 2$ and c is odd, then there is also a $(v, k, \lambda/2)$ BIBD by Theorem 2.7 (3).

Proof. Let $\Phi \leq E^*$ be such that $|\Phi| = c$. It is clear that $S_0 \leq \tilde{0}$ and $\Phi \leq Stab_{F^*}(S)$. First we claim $\tilde{0} = S_0$. Suppose $a \in \tilde{0}$, We then have a is in the vector space over E with the basis $\{e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+d}\}$. Consider all elements of S in the following form $y = \beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_m e_m$. We know that $y + a \in S$ for any such y. Suppose α_i is the coefficient of e_i in a. Then we have $S_i + \alpha_i = S_i$ for any i with $1 \le i \le m$. By the second property of S_i, we get α_i must be 0 for $1 \le i \le m$. Therefore $a \in S_0$. Next we claim $Stab_{F^*}(S) = \Phi$. Note that $Stab_{F^*}(S) \le Stab_{F^*}(\tilde{0}) = Stab_{F^*}(S_0) = E^*$. Let $b \in Stab_{F^*}(S)$, then $b \in E^*$. For any element $z = r_1 e_1 + r_2 e_2 + \cdots + r_m e_m$ in the vector space over E with the basis $\{e_1, \ldots, e_m\}$, we have $bz \in S$. Therefore $br_i \in S_i$ for any $r_i \in S_i$ ($1 \le i \le m$); that means $b \in Stab_{F^*}(S_i) = \Phi_i$ for $1 \le i \le m$. We then get $b \in \Phi$ since Φ is the intersection of all Φ_i. Hence S generates a simple BIBD with the stated parameters. ∎

For the second requirement of S_i in the above theorem, it is enough to make sure that S_i is not a union of some cosets of a nontrivial additive subgroup of E. In most situations it is this case since the first requirement tells that $Stab_{F^*}(S_i)$ is nontrivial. Thus S_i always meets the second requirement if S_i is a ZSGB with trivial $\sim_r$ for S_i. Therefore combining this result with those in section three, we have the following consequence.

Theorem 4.17. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d and m be any number such that $d + m \le \alpha/\beta$. Suppose there are c_i, $1 \le i \le m$, such that c_i divides $p^{\beta} - 1$ and $\gcd(c_1, c_2, \ldots, c_m) = c \ne 1$. Suppose there are k_i, $1 \le i \le m$, such that $p \nmid k_i$ and one of the following situations holds:*

(1) $2 \le k_i \le p^{\beta} - 3$ *and* c_i *divides* k_i*;*

(2) $3 \le k_i \le p^{\beta} - 2$ *and* c_i *divides* $k_i - 1$.

Then there exists a simple BIBD with parameters $v = p^{\alpha}$, $k = k_1 k_2 \cdots k_m p^{\beta d}$, and $\lambda = k_1 k_2 \cdots k_m (k_1 k_2 \cdots k_m p^{\beta d} - 1)/c$. The BIBD is of the refined second-type if c divides $k_i - 1$ for every i; otherwise, it is of the refined first-type. If $p \ne 2$ and c is odd, then there is also a $(v, k, \lambda/2)$ BIBD.

Proof. Let us continue from the previous proof. For any $1 \le i \le m$, by the method in section three, we can construct first-type ZSGBO $S_i \subset E$ such that $Stab_{F^*}(S_i) = \Phi_i$ if c_i divides k_i; while we can construct second-type ZSGBO $S_i \subset E$ such that $Stab_{F^*}(S_i) = \Phi_i$ if c_i divides $k_i - 1$. The $\sim_r$ for S_i is always trivial since $p \nmid k_i$. Therefore the statement follows. ∎

In fact, the requirement $p \nmid k_i$ is not necessary as long as there is a refined-type ZSGB S_i such that $|S_i| = k_i$, $Stab_{F^*}(S_i) = \Phi_i$, and $\sim_r$ is trivial for S_i.

Corollary 4.18. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d and m be any number such that $d + m \leq \alpha/\beta$. Suppose there are c_i, $1 \leq i \leq m$, such that c_i divides $p^{\beta} - 1$ and $\gcd(c_1, c_2, \ldots, c_m) = c \neq 1$. Then there is a refined first-type BIBD with parameters $v = p^{\alpha}$, $k = c_1 c_2 \cdots c_m p^{\beta d}$, and $\lambda = c_1 c_2 \cdots c_m (c_1 c_2 \cdots c_m p^{\beta d} - 1)/c$. If $p \neq 2$ and c is odd, then there is also a $(v, k, \lambda/2)$ BIBD.*

Proof. Let $S = \Phi_1 e_1 + \Phi_2 e_2 + \cdots + \Phi_m e_m + S_0$, where $|\Phi_i| = c_i$. ■

Corollary 4.19. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d be any number such that $d < \alpha/\beta$. Suppose $c \neq 1$ and c divides $p^{\beta} - 1$. Then there is a $(p^{\alpha}, cp^{\beta d}, cp^{\beta d} - 1)$ BIBD. If $p \neq 2$ and c is odd, then there is also a $(v, k, \lambda/2)$ BIBD. Therefore λ_{min} is attained for $v = p^{\alpha}$ and $k = cp^{\beta d}$ if $\gcd(cp^{\beta d} - 1, p^{\alpha} - 1) = 1$ or if $\gcd(cp^{\beta d} - 1, p^{\alpha} - 1) = 2$.*

The parameters of this construction are the same as those of a near resolvable design (NRD). However, the construction is an example of a $(v, k, k-1)$ BIBD which is not a NRD, since $v \equiv 1 \pmod{k}$ is a necessary condition for the existence of a NRD.

For example, let $p = 2$, $\alpha = 6$, $\beta = 2$, $d = 1$, and $c = 3$, then there exists a $(64, 12, 11)$ BIBD, which attains λ_{min}.

Corollary 4.20. *Suppose β is a proper divisor of α and $p^{\beta} > 2$. Let d and m be any number such that $d + m \leq \alpha/\beta$. Suppose there are c_i, $1 \leq i \leq m$, such that c_i is a proper divisor of $p^{\beta} - 1$, $p \nmid (c_i + 1)$, and $\gcd(c_1, c_2, \ldots, c_m) = c \neq 1$. Then there is a refined second-type BIBD with parameters $v = p^{\alpha}$, $k = (c_1 + 1)(c_2 + 1) \cdots (c_m + 1) p^{\beta d}$, and $\lambda = (c_1 + 1)(c_2 + 1) \cdots (c_m + 1)((c_1 + 1)(c_2 + 1) \cdots (c_m + 1) p^{\beta d} - 1)/c$.*

Proof. Let $S = (\Phi_1 \cup \{0\}) e_1 + (\Phi_2 \cup \{0\}) e_2 + \cdots + (\Phi_m \cup \{0\}) e_m + S_0$. ■

For example, let $p = 3$, $\alpha = 2h$ for $h \geq 2$, $\beta = 2$, $d = m = 1$, and $c = 4$, then there exists a $(9^h, 45, 55)$ BIBD.

Theorem 4.21. *Suppose $2 \leq d < \alpha$. Then there is a $(2^{\alpha}, 2^d, 2^d - 1)$ RBIBD, which is of the third-type. The design attains λ_{min} when $\gcd(d, \alpha) = 1$. In particular, it is an affine design if $d = \alpha - 1$. In this case any two blocks from distinct parallel classes intersect in $2^{\alpha - 2}$ points.*

Proof. Same ideas as those in Theorem 4.14 and Theorem 4.15. ■

Theorem 4.22. *Suppose β is a proper divisor of α. Let E be the subfield of F with $|E| = p^\beta$. Let $q' = p^\beta$, $n = \alpha/\beta$, and let d be any number less than n. Let $AG_d(n, q') = \{S + a \mid S$ is a d-dimensional vector subspace of F over E, $a \in F\}$, that is, the collection of all d-dimensional flats. We have that the block design $AG_d(n, q')$ is a disjoint union of RBIBDs.*

Proof. It follows from Theorem 4.15 and the above theorem. ■

We are going to construct more third-type BIBDs in the following part.

Lemma 4.23. *Suppose $q = 2^\alpha$ and $2 \le k < q$. Let $S \subset F$ with $|S| = k$. If $\gcd(k(k-1), q-1) = 1$, then the BIBD generated by S has parameters $(q, k, k(k-1)/h)$ where $h = |\tilde{0}|$.*

Proof. When $\gcd(k(k-1), q-1) = 1$, $\bar{1}$ is trivial according to Corollary 4.8. ■

Theorem 4.24. *Suppose $d \ge 1$, $\ell \ge 3$, $\ell 2^d < 2^\alpha$, and $\gcd(\ell(\ell 2^d - 1), 2^\alpha - 1) = 1$. Then there is a $(2^\alpha, \ell 2^d, \ell(\ell 2^d - 1))$ simple BIBD whenever (1) ℓ is odd; or (2) ℓ is even and $\ell \le \sqrt{2^{\alpha-d+2} + 4} - 4$. We further have the following results.*

(1) *When 4 divides $\ell 2^d$, the constructed BIBD is of the third type.*
(2) *When $d = 1$ and ℓ is odd, the constructed BIBD is of the fourth type.*
(3) *The BIBD attains λ_{min} when ℓ is odd.*

Proof. Let $q = 2^\alpha$ and $k = \ell 2^d$. Let H be an additive subgroup with $|H| = 2^d$. We need a generating block $S = \sqcup_{i=1}^{\ell} (a_i + H)$ such that S is a disjoint union of additive cosets of H and $\tilde{0} = H$. How to choose this kind of S? When ℓ is odd, it is always this case. There are $\binom{2^{\alpha-d}}{\ell}$ choices. So we now suppose that ℓ is even. Let K be a $(d+1)$-dimensional vector subspace over Z_2 with $H \subset K$. Suppose $\{e_1, e_2, \ldots, e_\alpha\}$ is a basis of F over Z_2, where $\{e_1, e_2, \ldots, e_d\}$ is a basis of H over Z_2. Then we have exactly $2^{\alpha-d} - 1$ distinct K. This can be seen by making a basis $\{e_1, e_2, \ldots, e_d, a\}$ of K, where $a \ne 0$ is chosen from the vector subspace spanned by $\{e_{d+1}, e_{d+2}, \ldots, e_\alpha\}$. For each K, we have $\binom{2^{\alpha-d-1}}{\ell/2}$ distinct choices of S with $S + K = S$. Therefore, if $\binom{2^{\alpha-d}}{\ell} \ge 2^{\alpha-d}\binom{2^{\alpha-d-1}}{\ell/2}$, we can make sure that there exists S such that $\tilde{0} = H$. When is this inequality valid? Consider that

$$\binom{2^{\alpha-d}}{\ell} = \frac{2^{\alpha-d}(2^{\alpha-d}-1)\cdots(2^{\alpha-d}-\ell/2+1)(2^{\alpha-d}-\ell/2)(2^{\alpha-d}-\ell/2-1)\cdots}{1\cdot 2\cdots \ell/2(\ell/2+1)(\ell/2+2)\cdots}$$

and

$$\binom{2^{\alpha-d-1}}{\ell/2} = \frac{2^{\alpha-d-1}(2^{\alpha-d-1}-1)\cdots(2^{\alpha-d-1}-\ell/2+1)}{1\cdot 2\cdots \ell/2}.$$

Hence the inequality holds if $2^{\alpha-d}-\ell/2-1 \geq (\ell/2+1)(\ell/2+2)$ and $2^{\alpha-d}-\ell+1 \geq \ell$, which is equivalent to $\ell \leq \sqrt{2^{\alpha-d+2}+4}-4$. It is not difficult to assure the rest results. Note that when $d \geq 2$, S is a ZSGB by Theorem 4.3. When $d = 1$, S is a ZSGB if and only if 2 divides ℓ. ■

For example, take $\alpha = 5$, $d = 2$, and $\ell = 3$, we then have a $(32, 12, 33)$ third-type BIBD, which attains λ_{min}. For another example, take $\alpha = 7$, $d = 1$, and $\ell = 6$, we then obtain a $(128, 12, 66)$ third-type BIBD.

Sometimes we can have third-type BIBDs when $\gcd(k(k-1), 2^\alpha - 1) \neq 1$.

Theorem 4.25. *There is a* $(2^\alpha, 4\ell, 2\ell(4\ell-1))$ *third-type BIBD whenever* $\ell \leq \sqrt{2^{\alpha-1}+1}-2$.

Proof. Let $q = 2^\alpha$, $k = 4\ell$, and $H = \{0, 1\}$. We need a generating block $S = \sqcup_{i=1}^{2\ell}(a_i + H)$ such that S is a disjoint union of some additive cosets of H and $\tilde{0} = H$. Then we have $\overline{1}$ is trivial since $\overline{1} \leq Stab_{F^*}(\tilde{0})$ according to Theorem 4.11. Is there any S with the above properties? We can make sure of this by the same argument as in the proof of the above theorem. Let $\{e_1 = 1, e_2, \ldots, e_\alpha\}$ be a basis of F over Z_2. Therefore, if $\binom{2^{\alpha-1}}{2\ell} \geq 2^{\alpha-1}\binom{2^{\alpha-2}}{\ell}$, we can always have the required generating block. The inequality is valid if $2^{\alpha-1}-\ell-1 \geq (\ell+1)(\ell+2)$ and $2^{\alpha-1}-2\ell+1 \geq 2\ell$, which is equivalent to $\ell \leq \sqrt{2^{\alpha-1}+1}-2$. Hence the statement follows. ■

For example, take $\alpha = 6$ and $\ell = 2$, we then have a $(64, 8, 28)$ third-type BIBD. For another example, take $\alpha = 6$ and $\ell = 3$, we then obtain a $(64, 12, 66)$ third-type BIBD.

5. Conclusion and Remarks

In this article we point out that there are strong connections between the constructions of simple BIBDs from field-generated (or nearfield-generated) planar nearrings and the action of a sharply 2-transitive group on a set. In section two, we develop a method for constructing BIBDs, as summarized in Theorem 2.7. We analyze the structures of the constructions. In section three, we give the constructions from finite fields. We show that there exists a generating block S in the field F with respect to the given stabilizer $Stab_{F^*}(S)$, as indicated in Theorem 3.5. Accordingly, BIBDs with the possible parameters can be obtained in Corollary 3.6. Thereafter, we develop other constructions of BIBDs in section four, as indicated in Theorem 4.4, Theorem 4.10, and Theorem 4.14 to Theorem 4.25. Meanwhile, we classify the constructed BIBDs according to the types of the respective generating blocks. One significant result is that new series of resolvable BIBDs appear in Theorem 4.15 and Theorem 4.21. And, it is quite interesting that the BIBD from the collection of all d-dimensional flats is a disjoint union of resolvable BIBDs, mentioned in Theorem 4.22.

A big portion of simple BIBDs with various parameters are constructed in this article. Many simple BIBDs with the same parameters appear here. It might be interesting to investigate their differences, especially the isomorphism problems. We refer to a recent paper on this part [4], where the full automorphism group of certain designs can be determined.

After section two, it becomes clear that field-generated planar nearrings can be used to constructing BIBDs.

A *PBD* (*pairwise balanced design*) with parameters (v, K, λ), where K is a set of positive integers and λ is a positive integer, is a collection $\mathcal{B}$ of subsets (called blocks) of a v-set V such that

(1) $\{|B| \mid B \in \mathcal{B}\} = K$; and
(2) $|\{B \in \mathcal{B} \mid p, q \in B\}| = \lambda$ for any p, $q \in V$ with $p \neq q$.

Thus a BIBD is a PBD with $|K| = 1$.

Therefore, any collection of the same geometric objects, such as triangles, obtained from a field-generated planar nearring is a simple PBD, and it is also a disjoint union of simple BIBDs. In case every generating block of the BIBDs has the same block size, then the PBD becomes a BIBD naturally. The rest questions are then on what kind parameters the design can possess, like those developments in section three and section four.

For another viewpoint, Boykett and Mayr generalize the construction of BIBDs from planar nearrings using fixed-point-free automorphisms on a group and short difference families [7]. This explains why sometimes ring-generated (or nearfield-generated) planar nearrings can produce BIBDs.

By similar constructions, using finite rings with unit, PBIBDs (partially balanced incomplete block designs) can be obtained [22]. Therefore, ring-generated finite planar nearrings can be used for the construction of PBIBDs.

Acknowledgments

The author thanks the referees for reading this article, for correcting the errors, and for making suggestions.

References

1. M. Anshel and J. R. Clay, Planar algebraic systems: some geometric interpretations, *J. Algebra*, **10** (1968), 166-173.

2. M. Anshel and J. R. Clay, Planarity in algebraic systems, *Bull. Amer. Math. Soc.*, **74** (1968), 746-748.

3. K. I. Beidar, Y. Fong and W.-F. Ke, On finite circular planar nearrings, *J. Algebra*, **185** (1996), 688-709.

4. K. I. Beidar, W.-F. Ke, C.-H. Liu and W.-R. Wu, Automorphism groups of certain simple 2-(q,3,λ) designs constructed from finite fields, *Finite Fields Appl.*, **9** (2003), 400-412.

5. T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, second ed., Cambridge University Press, Cambridge, 1999.

6. R. Bose, On the construction of balanced incomplete block designs, *Annals of Eugenics*, **9** (1939), 353-399.

7. T. Boykett and P. Mayr, Difference methods and Ferrero pairs, in: *Proceedings of the 18th International Conference on Nearrings and Nearfields Hamburg*, H. Kiechle, A. Kreuzer and M. J. Thomsen (eds.), Germany, Springer, 2005, pp. 177-187.

8. J. R. Clay, Generating balanced incomplete block designs from planar near-rings, *J. Algebra*, **22** (1972), 319-331.

9. J. R. Clay, Circular block designs from planar nearrings, *Ann. Discrete Math.*, **37** (1988), 95-106.

10. J. R. Clay, Tactical configurations from a planar nearring can also generate balanced incomplete block designs, *J. Geom.*, **32** (1988), 13-20.

11. J. R. Clay, Geometric and combinatorial ideas related to circular planar nearrings, *Bull. Inst. Math. Acad. Sinica*, **16** (1988), 275-283.

12. J. R. Clay, *Nearrings: Geneses and Applications*, Oxford University Press, Oxford, 1992.

13. J. R. Clay, Circular planar nearrings with application, in: *Proceedings of KAIST Math. Workshop*, 1992, pp. 149-177.

14. J. R. Clay, Geometry in fields, *Algebra Colloq.*, **1** (1994), 289-306.

15. G. Ferrero, Stems planari e BIB-desegni, *Riv. Mat. Univ. Parma*, (1970), 79-96.

16. R. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Annals of Eugenics*, **10** (1940), 52-75.

17. W.-F. Ke, *Structures of Circular Planar Nearrings*, Ph.D. Dissertation, University of Arizona, Tucson, 1992.

18. W.-F. Ke, On recent developments of planar nearrings, in: *Proceedings of the 18th International Conference on Nearrings and Nearfields Hamburg*, H. Kiechle, A. Kreuzer and M. J. Thomsen (eds.), Germany, Springer, 2005.

19. M. C. Modisett, *A Characterization of the Circularity of Certain Balanced Incomplete Block Designs*, Ph.D. Dissertation, University of Arizona, Tucson, 1988.

20. H.-M. Sun, *Planar Nearrings and Block Designs*, Ph.D. Dissertation, University of Arizona, Tucson, 1995.

21. H.-M. Sun, Segments in a planar nearring, *Discrete Math.*, **240** (2001), 205-217.

22. H.-M. Sun, PBIB designs and association schemes obtained from finite rings, *Discrete Math.*, **252** (2002), 267-277.

23. H. Wähling, *Theorie der Fastkörper*, Thales Verlag, Essen, 1987.

24. F. Yates, Incomplete randomized blocks, *Annals of Eugenics*, **7** (1936), 121-140.

Hsin-Min Sun
Department of Mathematics Education,
National University of Tainan,
Tainan 700, Taiwan
E-mail: sunhm@mail.nutn.edu.tw