On the Existence of $(v, 5, 1)$-BIBDs

Clayton Smith, ID# 98037331

February 23, 2004

1 Introduction

In this paper, we prove that a $(v, 5, 1)$-BIBD exists if and only if $v \equiv 1$ or 5 (mod 20).

In Section 2 we define the main concepts used throughout the paper, and establish some connections between them. In Sections 3 and 4 we describe the necessary direct and recursive constructions. These constructions are used in Section 5, where the main result is proven.

Throughout this paper, curly brackets will be used to denote sets, while square brackets will be used to denote multisets.

2 Definitions

Definition 1. *Let v, k, λ be positive integers satisfying $v > k \geq 2$. A (v, k, λ)-* balanced incomplete block design *or* BIBD *is a pair $(X, \mathcal{A})$ satisfying the following properties:*

1. *X is a set of v elements called* points*,*
2. *$\mathcal{A}$ is a collection of k-subsets of X called* blocks*, and*
3. *every pair of distinct points is contained in exactly λ blocks.*

Example 2. *The following is a $(9, 3, 1)$-BIBD:*

$$\begin{aligned} X &= \{1,2,3,4,5,6,7,8,9\} \\ \mathcal{A} &= [\{1,2,3\},\{4,5,6\},\{7,8,9\},\{1,4,7\},\{2,5,8\},\{3,6,9\}, \\ &\qquad \{1,5,9\},\{2,6,7\},\{3,4,8\},\{1,6,8\},\{2,4,9\},\{3,5,7\}]. \end{aligned}$$

Lemma 3. *In a (v, k, λ)-BIBD, each point occurs in exactly*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks.

Proof. We will count the number of pairs containing a point x in two ways. First, x occurs λ times with each of the other $v-1$ points, giving $\lambda(v-1)$ pairs. Now let r_x be the number of blocks in which x occurs. In each block, x occurs with $k-1$ other points, giving $r_x(k-1)$ pairs. Thus we have $r_x(k-1) = \lambda(v-1)$, which gives

$$r_x = \frac{\lambda(v-1)}{k-1}.$$

Note that this expression does not depend on x. □

The value r is called the *replication number* of the BIBD. In this paper, we consider $(v, 5, 1)$-BIBDs, for which $r = (v-1)/4$, i.e. $v = 4r + 1$.

Lemma 4. *Let $(X, \mathcal{A})$ be a (v, k, λ)-BIBD. Let r be its replication number, and let b be the number of blocks. Then*

$$b = \frac{\lambda v(v-1)}{k(k-1)}.$$

Proof. We simply count, with repetition, the number of points appearing in the blocks of the BIBD. First, there are b blocks each containing k points, giving bk. Also, there are v points each occurring r times, giving vr. Thus $bk = vr$. Then by Lemma 3 we have

$$\begin{aligned} bk &= \frac{\lambda v(v-1)}{k-1} \\ b &= \frac{\lambda v(v-1)}{k(k-1)}. \end{aligned}$$

□

These two lemmas provide us with necessary conditions for the existence of a (v, k, λ)-BIBD, as the following theorem shows.

Theorem 5. *Suppose there exists a (v, k, λ)-BIBD. Then $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.*

Proof. These conditions follow immediately from the fact that r and b from Lemmas 3 and 4 are integers. □

In this paper, we consider $(v, 5, 1)$-BIBDs, so these conditions become $v-1 \equiv 0 \pmod 5$ and $v(v-1) \equiv 0 \pmod{20}$. Solving these simultaneous equivalences, we get $v \equiv 1$ or $5 \pmod{20}$.

Definition 6. *Let $(G, +)$ be a finite group of order v with identity 0. Let k and λ be positive integers, and suppose $v > k \geq 2$. A (v, k, λ)*-difference family *or* DF *is a collection $[D_1, \ldots, D_l]$ of k-subsets of G called* blocks *such that the multiset union*

$$\bigcup_{i=1}^{l} [x - y : x, y \in D_i, x \neq y]$$

contains every element of $G \setminus \{0\}$ exactly λ times.

Example 7. *The following is a* $(13, 3, 1)$*-DF in* $(\mathbb{Z}_{13}, +)$*:*

$$[\{0, 1, 4\}, \{0, 2, 8\}].$$

Note that there are $v - 1$ possible differences each occurring λ times, while each block contributes $k(k - 1)$ differences. Thus the number of blocks is

$$l = \frac{\lambda(v - 1)}{k(k - 1)}.$$

Definition 8. *Let* $[D_1, \dots, D_l]$ *be a* (v, k, λ)*-DF in* $(G, +)$*. For any block* D_i *and group element* $g \in G$*, the set*

$$D_i + g = \{d + g : d \in D_i\}$$

is called a translate *of* D_i*. The* development *of* $[D_1, \dots, D_l]$ *is the collection of all translates of all blocks, i.e.*

$$\mathrm{Dev}(D_1, \dots, D_l) = [D_i + g : i \in \{1, \dots, l\}, g \in G].$$

Theorem 9. *Let* $[D_1, \dots, D_l]$ *be a* (v, k, λ)*-DF in an Abelian group* $(G, +)$*. Then* $(G, \mathrm{Dev}(D_1, \dots, D_l))$ *is a* (v, k, λ)*-BIBD.*

Proof. Properties 1 and 2 of Definition 1 are clearly satisfied. Thus it remains only to verify property 3. Choose $x, y \in G$ such that $x \neq y$. We must show that x and y occur together in exactly λ blocks of $(G, \mathrm{Dev}(D_1, \dots, D_l))$.

Let $d = x - y$. Clearly $d \neq 0$, so there are exactly λ pairs (x', y') such that $x', y' \in D_i$ for some i, and $x' - y' = d$. For each such pair, the translate $D_i + (x - x')$ contains $x' + (x - x') = x$ and $y' + (x - x') = y' + ((y - d) - (y' - d)) = y' + (y - y') = y$. In this process, no pair (x', i) can appear more than once, so we have found λ unique translates containing x and y.

By the above argument, each pair $x, y \in G$ with $x \neq y$ occurs in at least λ blocks of $(G, \mathrm{Dev}(D_1, \dots, D_l))$. There are $v(v - 1)/2$ such x, y, so there are at least $\lambda v(v - 1)/2$ pairs, counting with repetition. Each block contains $k(k - 1)/2$ pairs, so there are at least

$$\frac{\lambda v(v - 1)}{k(k - 1)}$$

blocks. Note that this is exactly the number of blocks in $\mathrm{Dev}(D_1, \dots, D_l)$. If any pair x, y occurred more than λ times, we would require additional blocks, a contradiction. Thus each pair x, y occurs in exactly λ blocks of $(G, \mathrm{Dev}(D_1, \dots, D_l))$, as required. □

Definition 10. *Let* $v \geq 2$ *be an integer. A* group-divisible design *or* GDD *is a triple* $(X, \mathcal{G}, \mathcal{B})$ *satisfying the following properties:*

1. X *is a set of* v *elements called* points*,*

2. $\mathcal{G}$ *is a partition of* X *into at least two nonempty subsets called* groups*,*

3. *$\mathcal{B}$ is a collection of subsets of X called* blocks, *where $|B| \geq 2$ for all $B \in \mathcal{B}$,*

4. *a group and a block contain at most one common point, and*

5. *every pair of points from distinct groups is contained in exactly one block.*

Example 11. *The following is a GDD:*

$X = \{2,3,4,5,6,7,8,9\}$
$\mathcal{G} = \{\{2,3\},\{4,7\},\{5,9\},\{6,8\}\}$
$\mathcal{B} = [\{4,5,6\},\{7,8,9\},\{2,5,8\},\{3,6,9\},\{2,6,7\},\{3,4,8\},\{2,4,9\},\{3,5,7\}].$

Theorem 12. *Suppose that $v > k \geq 2$. Then there exists a $(v,k,1)$-BIBD if and only if there exists a group-divisible design having $v-1$ points, $r = (v-1)/(k-1)$ groups of size $k-1$, and blocks of size k.*

Proof. "⇒": Suppose $(X, \mathcal{A})$ is a $(v,k,1)$-BIBD. Pick some point $x \in X$ and delete it from all blocks in which it appears. This will leave some blocks of size $k-1$ and some of size k. Let the blocks of size $k-1$ be the groups of the GDD, and the blocks of size k be the blocks of the GDD. That is, the new GDD is $(X \setminus \{x\}, \mathcal{G}, \mathcal{B})$, with

$$\mathcal{G} = \{A \setminus \{x\} : A \in \mathcal{A}, x \in A\}$$
$$\mathcal{B} = \{A : A \in \mathcal{A}, x \notin A\}.$$

Now we verify that $(X \setminus \{x\}, \mathcal{G}, \mathcal{B})$ is a GDD. Properties 1 and 3 of Definition 10 clearly hold. In the BIBD, the point x occurs exactly once with every point in $X \setminus \{x\}$, so $\mathcal{G}$ indeed partitions $X \setminus \{x\}$. The point x occurs in r blocks, so $\mathcal{G}$ contains r groups of size $k-1$. Since $v > k$, we have $r \geq 2$, so property 2 is satisfied. Since $\lambda = 1$, any two groups of the BIBD contain at most one common point. Thus a group and a block in the GDD contain at most one common point, satisfying property 4. Let y, z be two distinct points from $X \setminus \{x\}$. Certainly y and z occur together in a unique block $A \in \mathcal{A}$, and if y and z are from distinct groups then $x \notin A$, i.e. $A \in \mathcal{B}$. Thus A is the unique block in which y and z occur, so property 5 is satisfied.

"⇐": Now suppose that $(X, \mathcal{G}, \mathcal{B})$ is a GDD with the given properties. Suppose that $\infty \notin X$ and form a BIBD by adding the point ∞ to each of its groups, and letting the blocks of the BIBD be these augmented groups plus the blocks of the GDD. That is, the new BIBD is $(X \cup \{\infty\}, \mathcal{A})$, where

$$\mathcal{A} = \{G \cup \{\infty\} : G \in \mathcal{G}\} \cup \mathcal{B}.$$

Now we verify that $(X \cup \{\infty\}, \mathcal{A})$ is a BIBD. Properties 1 and 2 of Definition 1 clearly hold. Now suppose that x, y are distinct points from $X \cup \{\infty\}$. If one of x, y is ∞, then the other occurs in a unique group $G \in \mathcal{G}$, so the pair x, y occurs only in the block $G \cup \{\infty\} \in \mathcal{A}$. Otherwise both x and y are from X. If they are both from some group $G \in \mathcal{G}$, then they occur only in the block $G \cup \{\infty\} \in \mathcal{A}$. If they are from distinct groups, then they occur in a unique block $B \in \mathcal{B}$, and in no other block of $\mathcal{A}$. Thus property 3 is satisfied. □

As an example, if we take the BIBD from Example 2 and remove the point 1, we get the GDD from Example 11. Adding the point ∞ and renaming it to 1, we get back the original BIBD.

Definition 13. *Let $k \geq 2$ and $n \geq 1$ be integers. A* transversal design $\mathrm{TD}(k, n)$ *is a triple $(X, \mathcal{G}, \mathcal{B})$ satisfying the following properties:*

1. *X is a set of kn elements called* points*,*

2. *$\mathcal{G}$ is a partition of X into k subsets of size n called* groups*,*

3. *$\mathcal{B}$ is a set of k-subsets of X called* blocks*,*

4. *any group and any block contain exactly one common point, and*

5. *every pair of points from distinct groups is contained in exactly one block.*

Note that a transversal design is simply a special type of group-divisible design.

Example 14. *The following is a* $\mathrm{TD}(3, 2)$*:*

$$\begin{aligned} X &= \{1, 2, 3, 4, 5, 6\} \\ \mathcal{G} &= \{\{1, 2\}, \{3, 4\}, \{5, 6\}\} \\ \mathcal{B} &= \{\{1, 3, 5\}, \{1, 4, 6\}, \{2, 3, 6\}, \{2, 4, 5\}\}. \end{aligned}$$

The following theorem provides a very useful class of transversal designs. It is simply a restatement of Theorem 6.34 from Stinson [2] in terms of transversal designs.

Theorem 15 (MacNeish's Theorem). *Let n be a positive integer with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$, where the p_i's are distinct primes and $e_i \geq 1$ for all i. Let $k = \min\{p_i^{e_i} + 1 : 1 \leq i \leq l\}$. Then there exists a* $\mathrm{TD}(k, n)$*.*

We will make use of the following simple corollary later on.

Corollary 16. *If $n \equiv 1$ or $5 \pmod 6$ then there exists a* $\mathrm{TD}(6, n)$*.*

Proof. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$. Since $n \equiv 1$ or $5 \pmod 6$, n is not divisible by 2 or 3. Thus $p_i \geq 5$ for all i. Thus $p_i^{e_i} + 1 \geq 5^{e_i} + 1 \geq 5 + 1 = 6$ for all i, so by MacNeish's Theorem, there exists a $\mathrm{TD}(6, n)$. □

Another useful existence theorem is the following, which is given as Theorem 3.10 in Hanani [1]:

Theorem 17. *For all $n > 42$, there exists a* $\mathrm{TD}(5, n)$*.*

Finally, note that it is possible to make smaller transversal designs from larger ones, as the following theorem shows.

Theorem 18. *Suppose there exists a* $\mathrm{TD}(k, n)$*. Then there exists a* $\mathrm{TD}(k', n)$ *for all $2 \leq k' \leq k$.*

Proof. Simply delete all but k' blocks from the $\mathrm{TD}(k, n)$. □

There are many ways to make BIBDs from transversal designs. In this paper, we will make use of the following three.

Theorem 19. *If there exists a* $\mathrm{TD}(k, n)$ *and an* $(n, k, 1)$*-BIBD, then there exists a* $(kn, k, 1)$*-BIBD.*

Proof. Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}(k, n)$. Replace each group $G \in \mathcal{G}$ with an $(n, k, 1)$-BIBD on the point set G. We will check that the resulting design $(X, \mathcal{A})$ is a $(kn, k, 1)$-BIBD.

$(X, \mathcal{A})$ clearly satisfies properties 1 and 2 of Definition 1, so it remains only to verify property 3. Suppose $x, y \in X$ are distinct points. If x and y are from distinct groups of the transversal design, then they occur together in a unique block $B \in \mathcal{B}$, and cannot occur in any other block of $\mathcal{A}$. If x and y are both from some group $G \in \mathcal{G}$, then they occur together in a unique block B from the $(n, k, 1)$-BIBD on the point set G, and cannot occur in any other block of $\mathcal{A}$. Thus property 3 is satisfied. □

Theorem 20. *If there exists a* $\mathrm{TD}(k, n)$ *and an* $(n + 1, k, 1)$*-BIBD, then there exists a* $(kn + 1, k, 1)$*-BIBD.*

Proof. Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}(k, n)$, and suppose $\infty \notin X$. Replace each group $G \in \mathcal{G}$ with an $(n + 1, k, 1)$-BIBD on the point set $G \cup \{\infty\}$. We will check that the resulting design $(X \cup \{\infty\}, \mathcal{A})$ is a $(kn + 1, k, 1)$-BIBD.

$(X \cup \{\infty\}, \mathcal{A})$ clearly satisfies properties 1 and 2 of Definition 1, so it remains only to verify property 3. Suppose $x, y \in X \cup \{\infty\}$. If one of x, y is ∞, then the other occurs in a unique group $G \in \mathcal{G}$, and thus the pair x, y occurs in a unique block of the BIBD on $G \cup \{\infty\}$. Otherwise both x and y are from X. If they are both from the same group $G \in \mathcal{G}$, then the pair x, y occurs in a unique block of the BIBD on $G \cup \{\infty\}$. If they are from distinct groups, then they occur in a unique block $B \in \mathcal{B}$ and in no other block of $\mathcal{A}$. Thus property 3 is satisfied. □

Theorem 21. *If there exists a* $\mathrm{TD}(k, n)$ *and an* $(n + k, k, 1)$*-BIBD, then there exists a* $(kn + k, k, 1)$*-BIBD.*

Proof. Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}(k, n)$, and suppose $\infty_1, \ldots, \infty_k$ are distinct points not in X. Replace each group $G \in \mathcal{G}$ with an $(n + k, k, 1)$-BIBD on $G \cup \{\infty_1, \ldots, \infty_k\}$ in which one of the blocks is $\{\infty_1, \ldots, \infty_k\}$. Finally, remove all but one of the copies of $\{\infty_1, \ldots, \infty_k\}$ to get the design $(X \cup \{\infty_1, \ldots, \infty_k\}, \mathcal{A})$. We will check that this is a BIBD.

$(X \cup \{\infty_1, \ldots, \infty_k\}, \mathcal{A})$ clearly satisfies properties 1 and 2 of Definition 1, so it remains only to verify property 3. Suppose $x, y \in X \cup \{\infty_1, \ldots, \infty_k\}$ are distinct points. If both x and y are in $\{\infty_1, \ldots, \infty_k\}$, then they occur together only in the block $\{\infty_1, \ldots, \infty_k\} \in \mathcal{A}$. If exactly one of x, y is in $\{\infty_1, \ldots, \infty_k\}$ then the other occurs in a unique group $G \in \mathcal{G}$, and thus the pair occurs in a unique block of the BIBD on $G \cup \{\infty_1, \ldots, \infty_k\}$. Otherwise both x and y are from X. If they are both from the same group $G \in \mathcal{G}$, then the pair x, y occurs in a unique block of the BIBD on $G \cup \{\infty_1, \ldots, \infty_k\}$. If they are from distinct groups, then they occur in a unique block $B \in \mathcal{B}$ and in no other block of $\mathcal{A}$. Thus property 3 is satisfied. □

Definition 22. *Suppose $v \geq 2$ and $\lambda \geq 1$ are integers, and $K \subseteq \{n \in \mathbb{Z} : n \geq 2\}$. A (v, K)-*pairwise balanced design *or PBD is a pair $(X, \mathcal{A})$ satisfying the following properties:*

1. *X is a set of v elements called* points*,*
2. *$\mathcal{A}$ is a collection of subsets of X called* blocks*, with $|A| \in K$ for each $A \in \mathcal{A}$, and*
3. *every pair of distinct points is contained in exactly λ blocks.*

Note that every $(v, k, 1)$-BIBD is a $(v, \{k\})$-PBD. Pairwise balanced designs can also be constructed from transversal designs, as the following theorem shows.

Theorem 23. *Suppose there is a* $\mathrm{TD}(k+1, t)$*, with $k \geq 2$. Then the following pairwise balanced designs exist:*

1. *a $(kt, \{k, t\})$-PBD,*
2. *a $(kt+1, \{k, k+1, t\})$-PBD,*
3. *a $(kt+u, \{k, k+1, t, u\})$-PBD for all u such that $2 \leq u \leq t-1$, and*
4. *a $(kt+t, \{k+1, t\})$-PBD.*

Proof. To prove 4, simply take all the blocks and groups of a $\mathrm{TD}(k+1, t)$ to be the blocks of a PBD. To prove 3, take a $\mathrm{TD}(k+1, t)$ and delete $t-u$ blocks from one group. Then take all the resulting blocks and groups to be the blocks of a PBD. To prove 2, take a $\mathrm{TD}(k+1, t)$ and delete $t-1$ blocks from one group. Take all the resulting blocks and groups, except the group of size 1, to be the blocks of a PBD. To prove 1, take a $\mathrm{TD}(k+1, t)$ and delete one entire group. Then take the resulting blocks and groups to be the blocks of a PBD.

Now let $(X, \mathcal{G}, \mathcal{B})$ be the original $\mathrm{TD}(k+1, t)$, and let $(Y, \mathcal{A})$ be the resulting design. We would like to verify that $(Y, \mathcal{A})$ is a PBD. In each of the four cases, it is clear that properties 1 and 2 of Definition 22 are satisfied. Now suppose that $x, y \in Y \subseteq X$ are distinct points. If they are both from the same group $G \in \mathcal{G}$, then they occur together only in the corresponding block $G' \in \mathcal{A}$, where $G' \subseteq G$. (G' is either G itself or the result of truncating G.) If they are from distinct groups, then they occur in a unique block $B \in \mathcal{B}$, and in no other group of $\mathcal{A}$. Thus property 3 is satisfied. □

3 Direct Constructions

Theorem 24. *If q is a prime power satisfying $q \equiv 1 \pmod 4$, then there exists a group-divisible design with q groups of size 5, and blocks of size 5.*

Proof. Let α be a primitive root of $\mathrm{GF}(q)$, and let $d = (q-1)/4$. Then define

$$\begin{aligned} X &= \mathbb{Z}_5 \times \mathrm{GF}(q) \\ G_\beta &= \mathbb{Z}_5 \times \{\beta\} \\ \mathcal{G} &= \{G_\beta : \beta \in \mathrm{GF}(q)\} \\ B_{ij\beta} &= \{(i,\beta), (i+1, \alpha^j + \beta), (i+1, \alpha^{j+2d} + \beta), \\ &\qquad (i-1, \alpha^{j+d} + \beta), (i-1, \alpha^{j+3d} + \beta)\} \\ \mathcal{B} &= \{B_{ij\beta} : (i,j,\beta) \in \mathbb{Z}_5 \times \{0,1,\ldots,d-1\} \times \mathrm{GF}(q)\}. \end{aligned}$$

Note that since α has order $q-1 = 4d$, we must have $\alpha^{2d} = -1$, and thus the blocks may be rewritten as

$$\begin{aligned} B_{ij\beta} = \{&(i,\beta), (i+1, \alpha^j + \beta), (i+1, -\alpha^j + \beta), \\ &(i-1, \alpha^{j+d} + \beta), (i-1, -\alpha^{j+d} + \beta)\} \end{aligned} \tag{1}$$

Now we must verify properties 4 and 5 of Definition 10.

Note that $0 \le j, j+2d, j+d, j+3d \le q-2$. Then since α has order $q-1$, we see that $\alpha^j, \alpha^{j+2d}, \alpha^{j+d}$ and α^{j+3d} are all distinct, and of course different from 0. Thus $\beta, \alpha^j + \beta, \alpha^{j+2d} + \beta, \alpha^{j+d} + \beta$ and $\alpha^{j+3d} + \beta$ are all distinct. Thus no block contains two elements from the same group, so property 4 is satisfied.

Suppose (a_1, γ_1) and (a_2, γ_2) are points from distinct groups, i.e. $\gamma_1 \neq \gamma_2$. We must show that these points are contained in a unique block $B_{ij\beta}$. There are three cases to consider, depending on the value of $a_1 - a_2$:

1. If $a_1 - a_2 = 0$, i.e. $a_1 = a_2$ then from (1) we must have either

$$\{(a_1,\gamma_1), (a_2,\gamma_2)\} = \{(i+1, \alpha^j + \beta), (i+1, -\alpha^j + \beta)\} \tag{2}$$

   or

$$\{(a_1,\gamma_1), (a_2,\gamma_2)\} = \{(i-1, \alpha^{j+d} + \beta), (i-1, -\alpha^{j+d} + \beta)\}. \tag{3}$$

   In either case, adding the second coordinates gives $\gamma_1 + \gamma_2 = 2\beta$, which has a unique solution for β since 2 is invertible in $\mathrm{GF}(q)$ when q is odd. Subtracting the second coordinates gives four possibilities for $\gamma_1 - \gamma_2$, namely $2\alpha^j, -2\alpha^j$ $(= 2\alpha^{j+2d})$ from (2) and $2\alpha^{j+d}, -2\alpha^{j+d}$ $(= 2\alpha^{j+3d})$ from (3). Multiplying through by 2^{-1}, we see that there are four possibilities for $2^{-1}(\gamma_1 - \gamma_2)$, namely $\alpha^j, \alpha^{j+2d}, \alpha^{j+d}$ and α^{j+3d}. Note that for $j \in [0, d-1]$, these expressions produce every invertible element of $\mathrm{GF}(q)$ exactly once. Since $2^{-1}(\gamma_1 - \gamma_2)$ is invertible, j is uniquely determined. If $2^{-1}(\gamma_1 - \gamma_2)$ is of the form a^j or a^{j+2d} then (2) holds and $i = a_1 - 1$. Otherwise $2^{-1}(\gamma_1 - \gamma_2)$ is of the form a^{j+d} or a^{j+3d}, so (3) holds and $i = a_1 + 1$. Thus i is uniquely determined.

2. If $a_1 - a_2 = \pm 1$ then assume, without loss of generality, that $a_1 - a_2 = 1$. Then from (1) we must have either

$$\begin{aligned}(a_1, \gamma_1) &= (i+1, \alpha^j + \beta) \text{ or } (i+1, -\alpha^j + \beta)\\ (a_2, \gamma_2) &= (i, \beta)\end{aligned}$$

or

$$\begin{aligned}(a_1, \gamma_1) &= (i, \beta)\\ (a_2, \gamma_2) &= (i-1, \alpha^{j+d} + \beta) \text{ or } (i-1, -\alpha^{j+d} + \beta).\end{aligned}$$

This gives four possibilities for $\gamma_1 - \gamma_2$, namely $\alpha^j, -\alpha^j$ $(= \alpha^{j+2d})$ from the first case and $-\alpha^{j+d}$ $(= \alpha^{j+3d}), \alpha^{j+d}$ from the second case. As before, these expressions produce every invertible element of $\mathrm{GF}(q)$ exactly once. Since $\gamma_1 - \gamma_2$ is invertible, j is uniquely determined. If $\gamma_1 - \gamma_2$ is of the form a^j or a^{j+2d} then we are in the first case, giving $i = a_2$ and $\beta = \lambda_2$. Otherwise $\gamma_1 - \gamma_2$ is of the form a^{j+d} or a^{j+3d}, so we are in the second case, giving $i = a_1$ and $\beta = \lambda_1$. Thus i and β are uniquely determined.

3. If $a_1 - a_2 = \pm 2$ then assume, without loss of generality, that $a_1 - a_2 = 2$. Then from (1) we must have

$$\begin{aligned}(a_1, \gamma_1) &= (i+1, \alpha^j + \beta) \text{ or } (i+1, -\alpha^j + \beta)\\ (a_2, \gamma_2) &= (i-1, \alpha^{j+d} + \beta) \text{ or } (i-1, -\alpha^{j+d} + \beta),\end{aligned}$$

so i is uniquely determined. Now there are four cases to consider. We will consider the value of $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2)$ in each case.

   (a) If $\gamma_1 = \alpha^j + \beta$ and $\gamma_2 = \alpha^{j+d} + \beta$ then $\gamma_1 - \gamma_2 = \alpha^j - \alpha^{j+d} = \alpha^j(1 - \alpha^d)$. Multiplying through by $(1 - \alpha^d)^{-1}$ we get $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2) = \alpha^j$.

   (b) If $\gamma_1 = \alpha^j + \beta$ and $\gamma_2 = -\alpha^{j+d} + \beta$ then $\gamma_1 - \gamma_2 = \alpha^j + \alpha^{j+d} = -\alpha^{j+2d} + \alpha^{j+d} = \alpha^{j+d}(-\alpha^d + 1)$. Multiplying through by $(1 - \alpha^d)^{-1}$ we get $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2) = \alpha^{j+d}$.

   (c) If $\gamma_1 = -\alpha^j + \beta$ and $\gamma_2 = \alpha^{j+d} + \beta$ then $\gamma_1 - \gamma_2 = -\alpha^j - \alpha^{j+d} = -\alpha^{j+4d} + \alpha^{j+3d} = \alpha^{j+3d}(-\alpha^d + 1)$. Multiplying through by $(1 - \alpha^d)^{-1}$ we get $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2) = \alpha^{j+3d}$.

   (d) If $\gamma_1 = -\alpha^j + \beta$ and $\gamma_2 = -\alpha^{j+d} + \beta$ then $\gamma_1 - \gamma_2 = -\alpha^j + \alpha^{j+d} = \alpha^{j+2d} - \alpha^{j+3d} = \alpha^{j+2d}(1 - \alpha^d)$. Multiplying through by $(1 - \alpha^d)^{-1}$ we get $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2) = \alpha^{j+2d}$.

   As before, these four expressions produce every invertible element of $\mathrm{GF}(q)$ exactly once. Since $(1 - \alpha^d)^{-1}(\gamma_1 - \gamma_2)$ is invertible, j is uniquely determined and exactly one of (a) through (d) holds, uniquely determining β.

The above discussion shows that property 5 is satisfied. □

Corollary 25. *If q is a prime power satisfying $q \equiv 1 \pmod 4$, then there exists a $(5q, 5, 1)$-BIBD.*

Proof. By Theorem 24 there exists a group-divisible design $(X, \mathcal{G}, \mathcal{B})$ with q groups of size 5, and blocks of size 5. Then $(X, \mathcal{G} \cup \mathcal{B})$ is a $(5q, 5, 1)$-BIBD. To see this, note that properties 1 and 2 of Definition 1 clearly hold. Now suppose x, y are distinct points from X. If they are both from the same group $G \in \mathcal{G}$, then they occur only in the block $G \in \mathcal{A}$. If they are from distinct groups, then they occur in a unique block $B \in \mathcal{B}$, so they occur only in the block $B \in \mathcal{A}$. Thus property 3 is satisfied. □

4 Recursive Constructions

Theorem 26. *If there exists an (n, M)-PBD and a $((k-1)m+1, k, 1)$-BIBD for each $m \in M$, then there exists a $((k-1)n+1, k, 1)$-BIBD.*

Proof. Let $(X, \mathcal{A})$ be an (n, M)-PBD. For each block $A \in \mathcal{A}$, we have $|A| \in M$, so there exists a $((k-1)|A|, k, 1)$-BIBD. Then by Theorem 12 there exists a GDD having $(k-1)|A|$ points, $|A|$ groups of size $k-1$, and blocks of size k. Let $I = \{1, 2, \ldots, k-1\}$, and construct this GDD on $A \times I$, where the groups are $\{x\} \times I$ for all $x \in A$. Let $\mathcal{B}_A$ be the blocks of this GDD. Now define

$$\begin{aligned} Y &= X \times I \\ \mathcal{H} &= \{\{x\} \times I : x \in X\} \\ \mathcal{B} &= \bigcup_{A \in \mathcal{A}} \mathcal{B}_A. \end{aligned}$$

We will show that $(Y, \mathcal{H}, \mathcal{B})$ is a GDD having $(k-1)n$ points, n groups of size $k-1$, and blocks of size k. Properties 1, 2 and 3 of Definition 10 clearly hold, so it remains only to check properties 4 and 5.

Choose any $H \in \mathcal{H}$ and $B \in \mathcal{B}$. Then $H = \{x\} \times I$ for some $x \in X$, and $B \in \mathcal{B}_A$ for some $A \in \mathcal{A}$. If $x \in A$ then H and B have at most one point in common, since $(A \times I, \{\{x\} \times I : x \in A\}, \mathcal{B}_A)$ is a GDD. If $x \notin A$ then H and B have no points in common, since B contains only points in $A \times I$. Thus property 4 is satisfied.

Choose any two points $(x, i), (y, j) \in X \times I$ from distinct groups. Since they are in distinct groups, we know $x \neq y$. Since $(X, \mathcal{A})$ is a PBD, there is a unique block $A \in \mathcal{A}$ such that $x, y \in A$. Then since $(A \times I, \{\{x\} \times I : x \in A\}, \mathcal{B}_A)$ is a GDD, there is a unique block $B \in \mathcal{B}_A$ such that $(x, i), (y, j) \in B$. Thus B is the unique block of $(Y, \mathcal{H}, \mathcal{B})$ which contains (x, i) and (y, j), so property 5 is satisfied.

Now we simply apply Theorem 12 to $(Y, \mathcal{H}, \mathcal{B})$ to get a $((k-1)n+1, k, 1)$-BIBD, as required. □

5 Main Result

Recall that a $(v, 5, 1)$-BIBD must have $v \equiv 1$ or $5 \pmod{20}$, and its replication number is $r = (v-1)/4$. Since $v > k$, the smallest possible v is 21. Translating these facts into the language of replication numbers, we get that $r \equiv 0$ or $1 \pmod 5$ and $r \geq 5$. Define

$$R = \{r : \text{there exists a } (4r+1, 5, 1)\text{-BIBD}\}.$$

To show that there exists a $(v, 5, 1)$-BIBD whenever $v \equiv 1$ or $5 \pmod{20}$, it suffices to show that R contains all r satisfying $r \equiv 0$ or $1 \pmod 5$ and $r \geq 5$. We establish that result in this section.

Lemma 27. *$\{6, 11, 16, 21, 31, 36, 46, 51, 76, 101, 151\} \subseteq R$.*

Proof. Simply apply Corollary 25 using $q = 5, 9, 13, 17, 25, 29, 37, 41, 61, 81, 121$ to get $(v, 5, 1)$-BIBDs with $v = 25, 45, 65, 85, 125, 145, 185, 205, 305, 405, 605$. □

Lemma 28. *$\{5, 10, 15, 20, 40, 70\} \subseteq R$.*

Proof. For each r above, we exhibit a $(4r+1, 5, 1)$-DF in an Abelian group, from which a $(4r+1, 5, 1)$-BIBD can be constructed by Theorem 9. The first three were found by the author using a computer program, and the remainder are from Table 5.9 in Hanani [1].

- $[\{0, 1, 4, 14, 16\}]$ is a $(21, 5, 1)$-DF in $\mathbb{Z}_{21}$, so $5 \in R$.
- $[\{0, 1, 4, 11, 29\}, \{0, 2, 8, 17, 22\}]$ is a $(41, 5, 1)$-DF in $\mathbb{Z}_{41}$, so $10 \in R$.
- $[\{0, 1, 3, 13, 34\}, \{0, 4, 9, 23, 45\}, \{0, 6, 17, 24, 32\}]$ is a $(61, 5, 1)$-DF in $\mathbb{Z}_{61}$, so $15 \in R$.
- The collection

$$\begin{aligned}[&\{(0,0,0,1), (2,0,0,1), (0,0,2,1), (1,2,0,2), (0,1,1,1)\},\\ &\{(0,0,1,0), (1,1,0,2), (0,2,1,0), (1,2,0,1), (1,1,1,0)\},\\ &\{(2,2,1,1), (1,2,2,2), (2,0,1,2), (0,1,2,1), (1,1,0,0)\},\\ &\{(0,2,0,2), (1,1,0,1), (1,2,1,2), (1,2,1,0), (0,2,1,1)\}]\end{aligned}$$

  is an $(81, 5, 1)$-DF in $(\mathbb{Z}_3)^4$, so $20 \in R$.
- The collection

$$\begin{aligned}[&\{(0,0), (1,1), (3,4), (4,16), (6,2)\},\\ &\{(0,0), (2,1), (6,4), (1,16), (5,2)\},\\ &\{(0,0), (4,1), (5,4), (2,16), (3,2)\},\\ &\{(0,0), (1,22), (3,19), (4,7), (6,21)\},\\ &\{(0,0), (2,22), (6,19), (1,7), (5,21)\},\\ &\{(0,0), (4,22), (5,19), (2,7), (3,21)\},\\ &\{(0,10), (0,13), (1,0), (2,0), (4,0)\},\\ &\{(0,0), (0,2), (0,8), (0,9), (0,13)\}]\end{aligned}$$

is a $(161, 5, 1)$-DF in $\mathbb{Z}_7 \times \mathbb{Z}_{23}$, so $40 \in R$.

- $[\{3^{2\alpha}, 3^{2\alpha+56}, 3^{2\alpha+112}, 3^{2\alpha+168}, 3^{2\alpha+224}\} : \alpha \in \{0, 1, \ldots, 13\}]$ is a $(281, 5, 1)$-DF in $\mathbb{Z}_{281}$, so $70 \in R$.

□

Lemma 29. $\{41, 45, 50, 71, 75, 100, 105, 106\} \subseteq R$.

Proof. We simply construct the corresponding BIBDs using constructions from sections 2 and 4.

- By Lemma 28, $10 \in R$, so there is a $(41, 5, 1)$-BIBD, i.e. a $(41, \{5\})$-PBD. Also $5 \in R$, so there is a $(21, 5, 1)$-BIBD. Thus by Theorem 26, there is a $(165, 5, 1)$-BIBD, i.e. $41 \in R$.
- By Lemma 27, $11 \in R$, so there is a $(45, 5, 1)$-BIBD, i.e. a $(45, \{5\})$-PBD. As above, there is a $(21, 5, 1)$-BIBD. Thus by Theorem 26, there is a $(181, 5, 1)$-BIBD, i.e. $45 \in R$.
- By Theorem 15, there is a TD$(5, 40)$. As above, there is a $(41, 5, 1)$-BIBD. Thus by Theorem 20, there is a $(201, 5, 1)$-BIBD, i.e. $50 \in R$.
- By Theorem 15, there is a TD$(5, 56)$. By Theorem 28, $15 \in R$, so there is a $(61, 5, 1)$-BIBD. Thus by Theorem 21, there is a $(285, 5, 1)$-BIBD, i.e. $71 \in R$.
- By Theorem 17, there is a TD$(5, 60)$. As above, there is a $(61, 5, 1)$-BIBD. Thus by Theorem 20, there is a $(301, 5, 1)$-BIBD, i.e. $75 \in R$.
- By Theorem 15, there is a TD$(5, 80)$. By Lemma 28, $20 \in R$, so there is an $(81, 5, 1)$-BIBD. Thus by Theorem 20, there is a $(401, 5, 1)$-BIBD, i.e. $100 \in R$.
- By Theorem 15, there is a TD$(5, 84)$. By Lemma 27, $21 \in R$, so there is an $(85, 5, 1)$-BIBD. Thus by Theorem 20, there is a $(421, 5, 1)$-BIBD, i.e. $105 \in R$.
- By Theorem 15, there is a TD$(5, 85)$. As above, there is an $(85, 5, 1)$-BIBD. Thus by Theorem 19, there is a $(425, 5, 1)$-BIBD, i.e. $106 \in R$.

□

Lemma 30. $35 \in R$.

Proof. A $(141, 5, 1)$-BIBD is given in Table 5.9 in Hanani [1], so $35 \in R$. □

Theorem 31. $R = \{r : r \equiv 0 \text{ } or \text{ } 1 \pmod 5), r \geq 5\}$.

Proof. We prove this statement by induction. Suppose that $r' \equiv 0$ or $1 \pmod 5$ and $r' \geq 5$. We would like to show that $r' \in R$, assuming that all smaller r are contained in R, i.e. $R' := \{r : r \equiv 0 \text{ or } 1 \pmod 5), 5 \leq r < r'\} \subseteq R$. There are three cases to consider:

1. If $r' \in \{5, 6, 10, 11, 15, 16, 20, 21, 31, 35, 36, 40, 41, 45, 46, 50, 51, 70, 71, 75, 76, 100, 101, 105, 106, 151\}$ then $r' \in R$ by Lemmas 27 through 30.

2. If $r' \in \{80, 81, 85, 86, 90, 91, 95, 96, 110, 111, 115, 116, 120, 121, 250, 251, 255, 256, 260, 261, 265, 266, 270, 271\}$ then apply Theorem 23 using the following values for k, t and u:

r'	k	t	u
$80 - 69$	5	16	$0 - 16$
$110 - 121$	10	11	$0 - 11$
$250 - 271$	10	25	$0 - 21$

   In each case, we know that a TD$(k+1, t)$ exists by Theorem 15 and Theorem 18. Since $k, k+1, t, u \in R'$, Theorem 23 gives us an (r', R')-PBD. Then by Theorem 26, there exists a $(4r'+1, 5, 1)$-BIBD, so $r' \in R$.

3. For all other r', apply Theorem 23 using $k = 5$, and t, u as in the following table. In each case we have $t \equiv 1$ or $5 \pmod 6$ so a TD$(6, t)$ exists by Corollary 16. We also have $t, u \equiv 0$ or $1 \pmod 5$, so $5, 6, t, u \in R'$. Thus Theorem 23 gives us an (r', R')-PBD. Then by Theorem 26, there exists a $(4r'+1, 5, 1)$-BIBD, so $r' \in R$.

   Note that to apply Theorem 23 we need $u \leq t$. This introduces some restrictions on s, which are listed in the table. The last column lists which values of r' cannot be dealt with using the table. These values are exactly the values that were dealt with in cases 1 and 2, so all possible values of r' have been covered.

r'	t	u	Restriction on s	Exceptions
$150s$	$30s-5$	25	$s \geq 1$	
$150s+1$	$30s-5$	26	$s \geq 2$	151
$150s+5$	$30s+1$	0	$s \geq 1$	5
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$150s+21$	$30s+1$	16	$s \geq 1$	21
$150s+25$	$30s+5$	0		
$150s+26$	$30s+5$	1		
$150s+30$	$30s+5$	5		
$150s+31$	$30s+5$	6	$s \geq 1$	31
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$150s+51$	$30s+5$	26	$s \geq 1$	51
$150s+55$	$30s+11$	0		
$\vdots$	$\vdots$	$\vdots$		
$150s+66$	$30s+11$	11		
$150s+70$	$30s+11$	15	$s \geq 1$	70
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$150s+96$	$30s+11$	41	$s \geq 1$	96
$150s+100$	$30s+11$	45	$s \geq 2$	$100, 250$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$150s+121$	$30s+11$	66	$s \geq 2$	$121, 271$
$150s+125$	$30s+25$	0		
$\vdots$	$\vdots$	$\vdots$		
$150s+146$	$30s+25$	21		

□

References

[1] H. Hanani. *Balanced incomplete block designs and related designs.* Discrete Mathematics, Vol. 11 (1975) pp. 255-369.

[2] Douglas R. Stinson. *Combinatorial Designs: Constructions and Analysis.* New York: Springer, 2003.