TAIWANESE JOURNAL OF MATHEMATICS
Vol. 20, No. 3, pp. 523–543, June 2016
DOI: 10.11650/tjm.20.2016.5021
This paper is available online at http://journal.tms.org.tw

More Results on the Existence of Simple BIBDs with Number of Elements a Prime Power

Hsin-Min Sun

Abstract. We study the existence of simple (q, k, λ) BIBDs when the number of elements is a prime power q and $\{c_1, c_2\} \cap \{1, 2\}$ is not empty, where $c_1 = \gcd(k, q-1)$ and $c_2 = \gcd(k-1, q-1)$. We show that in many situations the necessary conditions $\lambda(q-1) \equiv 0 \mod (k-1)$, $\lambda q(q-1) \equiv 0 \mod k(k-1)$, and $\lambda \leq \binom{q-2}{k-2}$ are also sufficient for the existence of a simple (q, k, λ) BIBD. These new results improve the valid range of simple BIBDs.

1. Introduction

The existence problem for combinatorial structures is among the main issues in combinatorics. In this paper, we will obtain some existence theorems for simple BIBDs whose number of elements is a prime power.

Let V be a finite set of symbols, and suppose $\mathcal{B}$ is a collection of subsets of V. Then $(V, \mathcal{B})$ is called a (v, k, λ) *BIBD* (*balanced incomplete block design*) if there are parameters v, k, and λ with $v > k \geq 2$ such that the following properties are satisfied:

(1) $|V| = v$;

(2) every *block* in $\mathcal{B}$ has exactly k symbols;

(3) every pair of distinct symbols appears in exactly λ blocks.

Suppose $(V, \mathcal{B})$ is a (v, k, λ) BIBD, it holds that every symbol appears in exactly r blocks, where $r = \lambda(v-1)/(k-1)$, and $b = |\mathcal{B}| = vr/k$. So sometimes a BIBD is described as a (v, b, r, k, λ) design. A design without repeated blocks is called *simple*.

Let v, k, and λ with $v > k \geq 2$ be positive integers. It is known 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).

Received July 3, 2014, accepted January 4, 2016.
Communicated by Xuding Zhu.
2010 *Mathematics Subject Classification.* Primary 05B05; Secondary 12E20.
Key words and phrases. Balanced incomplete block design, Finite field, Generating block.

We fix v and k, then the smallest positive integer λ that satisfies these conditions is denoted by $\lambda_{\min}$. It then follows that $\lambda_{\min}$ divides λ whenever a (v,k,λ) BIBD exists. Note that

$$\begin{aligned}\lambda_{\min} &= \operatorname{lcm}(\lambda_1,\lambda_2) = \frac{k(k-1)}{\gcd(k\gcd(k-1,v-1),\gcd(k(k-1),v(v-1)))}\\ &= \frac{k(k-1)}{c_1c_2\gcd(k,v)}\end{aligned}$$

where $\lambda_1=(k-1)/\gcd(k-1,v-1)$, $\lambda_2=k(k-1)/\gcd(k(k-1),v(v-1))$, $c_1=\gcd(k,v-1)$, and $c_2=\gcd(k-1,v-1)$. When v is a prime power $q=p^\alpha$ with $p\nmid k$, we obtain $\lambda_{\min}=k(k-1)/(c_1c_2)$; especially, if $\{c_1,c_2\}\cap\{1,2\}$ is not empty, then a simple $(q,k,\lambda_{\min})$ BIBD always exists[1].

Recent results [6,7] tell that, when the number of elements is a prime power q, in many situations the necessary conditions

(1) $\lambda(q-1)\equiv 0 \mod (k-1)$,

(2) $\lambda q(q-1)\equiv 0 \mod k(k-1)$, and

(3) $\lambda\le\binom{q-2}{k-2}$

are also sufficient for the existence of a simple (q,k,λ) BIBD. Here we continue the investigation, and the raised problem is: *For which specific q and block size k, it happens that all simple BIBDs whose parameters (q,k,λ) satisfy the necessary conditions exist?* We will introduce the new results (Theorems 2.1–2.8) in the next section, and give the proofs in Section 3. For terminologies and previously known results, the reader is referred to [1,2,5–7]. We review some facts in the rest part of this section.

BIBDs can be constructed by various ways. One of the methods uses difference families. Suppose $(V,+)$ is a group of order v. Let $B=\{b_1,b_2,\dots,b_k\}$ be a subset of V. The *V-stabilizer* of B is the subgroup $\operatorname{Stab}_V(B)$ of V consisting of all elements $g\in V$ such that $B+g=B$. B is *full* or *short* according to whether $\operatorname{Stab}_V(B)$ is or is not trivial. The *V-orbit* of B is the set $\operatorname{Orb}_V(B)$ of all distinct translates of B, namely, $\operatorname{Orb}_V(B)=\{B+s\mid s\in D\}$ where D is a complete system of representatives for the cosets of $\operatorname{Stab}_V(B)$ in V. The *list of differences from B* is the multiset $\Delta B=\{b_i-b_j\mid i,j=1,2,\dots,k;i\ne j\}$. The multiplicity in ΔB of an element $g\in V$ is of the form $\mu_g|\operatorname{Stab}_V(B)|$ for some integer μ_g. The *list of partial differences from B* is the multiset ∂B where each $g\in V$ appears

[1]This fact can be obtained directly from Theorem 1.2, according to the following situations:

(1) when $\{c_1,c_2\}=\{1,c\}$, at this time $\lambda_{\min}=k(k-1)/c$;

(2) when $p\ne 2$ and $\{c_1,c_2\}=\{c,2\}$, at this time $\lambda_{\min}=k(k-1)/(2c)$.

exactly μ_g times. Note that $\Delta B = \partial B$ if and only if B is a full block. A collection $\{B_1, \ldots, B_t\}$ of k-subsets of V forms a (v, k, λ) *difference family* if every nonzero element of V appears exactly λ times in $\partial B_1 \cup \cdots \cup \partial B_t$. The sets B_i are called *base blocks*. At this time the collection of blocks $\mathrm{Orb}_V(B_1) \cup \cdots \cup \mathrm{Orb}_V(B_t)$ forms a (v, k, λ) BIBD. A difference family having at least one short block is further called a *partial difference family*.

Let $(F, +, \cdot)$ be a finite field with $|F| = q = p^\alpha$. The action of the affine group $\mathrm{Aff}(F)$ on the complete design $\binom{F}{k}$ gives a partition of $\binom{F}{k}$, where

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

and $\binom{F}{k}$ is the collection of all k-subsets of F. Each orbit is a simple BIBD. That is, let S be any proper subset of F and $|S| = k \geq 2$. We call S a *generating block*. Define $\mathcal{B} = \{bS + a \mid b \in F^*,\ a \in F\}$, which is exactly the orbit $\mathrm{Orb}_G(S)$ of S under the action of the affine group $G = \mathrm{Aff}(F)$. Define an equivalence relation $\sim_c$ on F^* by $b_1 \sim_c b_2$ if there is an $a \in F$ such that $b_1 S = b_2 S + a$. Let $n = |F^*/\sim_c|$, and denote the equivalence class of b by $\overline{b}$. Define an equivalence relation $\sim_r$ on F by $a_1 \sim_r a_2$ if $S + a_1 = S + a_2$. Let $\mu = |F/\sim_r|$. We have the following result.

Theorem 1.1. [5, 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) *Let $\{b_1, b_2, \ldots, b_n\}$ be a set of representatives of the equivalence classes induced by $\sim_c$. Then $\{b_1 S, b_2 S, \ldots, b_n S\}$ is a difference family if $\sim_r$ is trivial, and a partial difference family if $\sim_r$ is nontrivial.*

(3) *If $\mathrm{char}\, F \neq 2$ 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 $\lambda = \frac{\mu n k(k-1)}{2q(q-1)}$.*

The idea of zero-sum generating blocks gives more detailed description for the structures of the constructions. If $\sum_{x \in S} x = 0$, we say that S is a *zero-sum generating block* (abbreviated as ZSGB). Suppose S is a ZSGB. 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.

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*. For any BIBD $(F, \mathcal{B})$, 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.

Suppose p, i.e., $\operatorname{char} F$, does not divide the block size k. Then $\sim_r$ is trivial. At this time, we have that a BIBD (or a generating block) with block size k is either of the first type or of the second type [5, Theorem 2.8]. Let S be a ZSGB, then $\overline{1} = \operatorname{Stab}_{F^*}(S)$ [5, Theorem 2.10]. Therefore, $|\operatorname{Stab}_{F^*}(S)|$ divides k if S is of the first type. Also, $|\operatorname{Stab}_{F^*}(S)|$ divides $(k-1)$ if S is of the second type.

Theorem 1.2. [5, Theorem 3.5, Corollary 3.6] *We assume that p is a prime and $q = p^\alpha$. Let $(F, +, \cdot)$ be the finite field with $|F| = q$. For $3 \le k \le q-4$, there is a first-type ZSGBO S such that $|S| = k$ and $|\operatorname{Stab}_{F^*}(S)| = c$ 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 $4 \le k \le q-3$, there is a second-type ZSGBO S such that $|S| = k$ and $|\operatorname{Stab}_{F^*}(S)| = c$ where c is any divisor of $\gcd(k-1, q-1)$. The exceptions are when $(q,k,c) = (7,4,1)$ or $(9,5,1)$.*

When $p \nmid k$ in any of these cases, we obtain that $\{S, \gamma S, \ldots, \gamma^{((q-1)/c-1)} S\}$ is a difference family, where γ is a generator of F^*. The difference family produces a simple $(q, k, k(k-1)/c)$ BIBD. 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 $(q, k, k(k-1)/(2c))$.

Wilson gets the idea of blocks with evenly distributed differences [8]. Let $(F, +, \cdot)$ be a finite field with $|F| = q$. Let γ be a generator of F^*. If e divides $q-1$, let $h = (q-1)/e$, we write H^e for the subgroup of order h, i.e., $H^e = \langle \gamma^e \rangle$. Also let $H_i^e = H^e \cdot \gamma^i$ for $0 \le i \le e-1$. A list L of elements of F^* is called *evenly distributed* over the e-th power cosets $H_0^e, H_1^e, \ldots, H_{e-1}^e$ if there is ℓ with $\ell e = |L|$ and in each coset there are ℓ elements of L, counting multiplicities.

Theorem 1.3. [8] *As in the above settings. Let S be a k-set such that the difference list of S is evenly distributed over $H_0^e, H_1^e, \ldots, H_{e-1}^e$. Then $\ell e = k(k-1)$, and $\{\gamma^{ie} S \mid 0 \le i \le h-1\}$ is a (q, k, ℓ) difference family. If $2e \mid (q-1)$, then $\{\gamma^{ie} S \mid 0 \le i \le h/2 - 1\}$ is a $(q, k, \ell/2)$ difference family.*

Theorem 1.4. [6, Theorem 5] *Let $(F, +, \cdot)$ be a finite field with $|F| = q$. Suppose e divides $q-1$; let $h = (q-1)/e$. Suppose a k-subset S generates a BIBD $(F, \mathcal{B})$ with trivial $\sim_r$, by the action of the affine group $\operatorname{Aff}(F)$ on S. Let $c = |\overline{1}|$. Suppose S also generates a difference family by Wilson's method, with respect to the subgroup H^e of order h. Then, the BIBD constructed by Wilson's method is simple if and only if $\gcd(c, h) = 1$. At this time $(F, \mathcal{B})$ can be partitioned into d isomorphic BIBDs, where $d = n/h = e/c$ and $n = (q-1)/c$.*

For all (q, k, λ_i) BIBDs $(1 \le i \le t_k)$ obtained from the affine constructions, i.e., the action of the affine group $\operatorname{Aff}(F)$ on the complete design $\binom{F}{k}$, suppose

(1) $\mathcal{B}_i$ can be further partitioned into d_i isomorphic BIBDs by Wilson's method for $1 \le i \le w$, according to Theorem 1.3;

(2) $\mathcal{B}_{w+1}, \mathcal{B}_{w+2}, \ldots, \mathcal{B}_{w+h}$ are distinct from the above BIBDs and each can be partitioned into two isomorphic BIBDs, according to Theorem 1.1(3);

(3) $\mathcal{B}_{w+h+1}, \mathcal{B}_{w+h+2}, \ldots, \mathcal{B}_{t_k}$ are the rest of the BIBDs.

We then make a list Λ of numbers:

(1) first we put d_i copies of λ_i/d_i in Λ for $1 \le i \le w$;

(2) next we put two copies of $\lambda_{w+i}/2$ in Λ for $1 \le i \le h$;

(3) finally, we put one copy of λ_i in Λ for $w+h+1 \le i \le t_k$.

We can also have a list $(\mathcal{B}'_1, \mathcal{B}'_2, \ldots, \mathcal{B}'_t)$ of mutually disjoint simple BIBDs whose parameters correspond to those numbers in the list Λ, where $t = t_k - w + h + \sum_{i=1}^{w} d_i$. Then any simple (q, k, λ) BIBD exists whenever λ can be expressed as a sum of some numbers chosen from the list Λ. The BIBD is formed by taking union of the BIBDs which correspond to those selected numbers for the sum.

Theorem 1.5. [6, Theorem 10] *Suppose* $3 \le k \le q-3$ *and* $p \nmid k(k-1)$. *Suppose* $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_t)$ *is a list of parameters described above. Then, the necessary conditions are also sufficient for the existence of a simple* (q, k, λ) *BIBD if there is a sublist* Γ *of* Λ *with the following properties:*

(1) $\sum_{\tau \in \Gamma} \tau \ge k(k-1) - \lambda_{\min}$;

(2) *any* $i\lambda_{\min}$ *with* $\lambda_{\min} \le i\lambda_{\min} \le \sum_{\tau \in \Gamma} \tau$ *can be expressed as a sum of numbers chosen from* Γ.

Using this theorem, we obtain several existence theorems for simple BIBDs. We quote four results in the following.

Suppose c divides $q-1$ and Φ is a subgroup of F^* with $|\Phi| = c$. Let $t_1(k, c)$ denote the number of distinct first-type BIBDs in the affine constructions with block size k and $|\overline{1}| = c$. Similarly, let $t_2(k, c)$ denote the number of distinct second-type BIBDs with block size k and $|\overline{1}| = c$. Let $t(k, c)$ denote the number of distinct BIBDs with block size k and $|\overline{1}| = c$. Recall that when $p \nmid k$, we have $t(k, c) = t_1(k, c) + t_2(k, c)$.

In the remainder of this paper, we always let $c_1 = \gcd(k, q-1)$ and $c_2 = \gcd(k-1, q-1)$.

Theorem 1.6. [6, Theorem 14] *Suppose* $3 \le k \le q-3$ *and* $p \nmid k(k-1)$. *Suppose* $\{c_1, c_2\} \cap \{1, 2\}$ *is not empty. Except when* $(k, c_1, c_2) = (3, 3, 2)$ *or* $(q-3, 2, 3)$, *suppose there exists a set* D *of some divisors of* $c_1 c_2$ *with the following properties:*

(1) $\sum_{d\in D} d \geq c_1c_2 - 1$, *and*

(2) *every number* i *with* $1 \leq i \leq \sum_{d\in D} d$ *can be expressed as a sum of distinct elements chosen from* D.

When $k \neq 3, q-3$ *and* $\{c_1, c_2\} \cap \{1, 2\} = \{2\}$, *let* d_1 *be the odd value in* $\{c_1, c_2\}$, *we further require that* $t(k, d_1/d) \geq 2$ *for any* d *such that both* d *and* $2d$ *are in* D. *Then, the necessary conditions are also sufficient for the existence of a simple* (q, k, λ) *BIBD.*

Theorem 1.7. [6, Theorem 15] *Suppose* $3 \leq k \leq q-3$, $p \nmid k(k-1)$, *and* $\{c_1, c_2\} = \{2, \beta^m\}$, *where* $m \geq 1$ *and* β *is odd. Then, the necessary conditions are also sufficient for the existence of a simple* (q, k, λ) *BIBD if* $t(k, \beta^m) \geq \beta$. *In particular, this is the case if* $q > \beta^m(\sqrt{6\beta + 1/4} + 3/2)$ *and* $q - 3\beta^m \geq k \geq 3\beta^m$.

Theorem 1.8. [6, Theorem 16] *Suppose* $3 \leq k \leq q-3$, $p \nmid k(k-1)$, *and* $\{c_1, c_2\} = \{1, \beta^m\}$, *where* $m \geq 1$ *and* β *is even. Then, the necessary conditions are also sufficient for the existence of a simple* (q, k, λ) *BIBD if* $t(k, \beta^m) \geq \beta - 1$. *In particular, this is the case in any of the following situations:*

(1) $q \geq \beta^m(2\beta - 1) + 1$ *and* $q - 2\beta^m \geq k \geq 2\beta^m$;

(2) $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$ *and* $q - 3\beta^m \geq k \geq 3\beta^m$.

Theorem 1.9. [6, Theorem 17] [7] *Suppose* $3 \leq k \leq q - 3$, $p \nmid k(k - 1)$, *and* $\{c_1, c_2\} = \{1, 2\beta^m\}$ *with* $m \geq 1$. *Then, the necessary conditions are also sufficient for the existence of a simple* (q, k, λ) *BIBD in the following cases:*

(1) β *is odd and* $t(k, \beta^m) \geq (\beta - 1)/2$. *In particular, this is the case in any of the following situations:*

   (a) $q \geq \beta^{m+1} + \beta^m + 1$ *and* $k = 2\beta^m$, $2\beta^m + 1$, $q - 2\beta^m$, *or* $q - 2\beta^m - 1$;

   (b) $q > \beta^m(\sqrt{3\beta - 11/4} + 3/2)$ *and* $q - 3\beta^m > k > 3\beta^m$.

(2) β *is even and* $t(k, \beta^m) \geq (\beta - 2)/2$. *In particular, this is the case in any of the following situations:*

   (a) $q \geq \beta^{m+1} + 1$ *and* $k = 2\beta^m$, $2\beta^m + 1$, $q - 2\beta^m$, *or* $q - 2\beta^m - 1$;

   (b) $q > \beta^m(\sqrt{3\beta - 23/4} + 3/2)$ *and* $q - 3\beta^m > k > 3\beta^m$.

Remark 1.10. Theorem 1.5 is still valid if the assumption "$p \nmid k$" is used instead of "$p \nmid k(k - 1)$". The interesting point about the condition "$p \nmid k(k - 1)$" is that there is a one to one correspondence between second-type BIBDs of block size k and first-type BIBDs of block size $k - 1$ in the affine constructions [6, Theorem 7]. However, we do not

use this property in the proofs of Theorems 1.5–1.9. That is, the assumption "$p \nmid k(k-1)$" is more restrictive. We find that Theorems 1.6–1.9 are still true if we use the condition "$p \nmid k$ and $p \neq 2$" instead of "$p \nmid k(k-1)$".

Note that when β and m are specified in Theorems 1.7–1.9, there are only a finite number of unknown cases left, whose values q are below the valid bounds. Hence, in order to reduce the amount of the unknown cases, it is reasonable to make the lower bounds for q as small as possible.

In the next section, we will introduce more results, which can improve the valid range of simple BIBDs.

2. More existence theorems for simple BIBDs

We state the results first, and we prove their correctness in the next section. With a similar proof to that of Theorem 1.8, we obtain a result for $q = 2^\alpha$.

Theorem 2.1. *Let $q = 2^\alpha$. Suppose $3 \le k \le q-3$ is odd, and $\{c_1, c_2\} = \{1, \beta^m\}$, where $m \ge 1$ and $\beta \ge 3$. Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \beta^m) \ge \beta - 1$. In particular, this is the case if $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$ and $q - 3\beta^m \ge k \ge 3\beta^m$.*

For example, a simple $(256, 45, 132i)$ BIBD exists for any i with $1 \le i \le \binom{254}{43}/132$, using $\beta = 15$.

Theorem 2.2. *Let q be a power p^α of an odd prime and let $\beta \ge 3$. Suppose $3\beta^m \le k \le q - 3\beta^m$, $p \nmid k$, and $\{c_1, c_2\} = \{2, 3\beta^m\}$ with $m \ge 1$. Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \beta^m) \ge (\beta - 1)/2$. In particular, this is the case in any of the following situations:*

(1) *$q > \beta^m(\sqrt{3\beta - 3/4} + 3/2)$ and $k = 3\beta^m$, $3\beta^m + 1$, $q - 3\beta^m$, or $q - 3\beta^m - 1$;*

(2) *$q > \beta^m(\sqrt{3\beta - 11/4} + 3/2)$ and $q - 9\beta^m \ge k \ge 9\beta^m$.*

For example, a simple $(601, 75, 37i)$ BIBD exists for any i with $1 \le i \le \binom{599}{73}/37$.

Theorem 2.3. *Let q be a prime power p^α and let $\ell, \beta \ge 2$. Suppose $3 \le k \le q-3$, $p \nmid k$, and $\{c_1, c_2\} = \{1, \ell\beta^m\}$ with $m \ge 1$. Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \ell\beta^m) \ge \ell - 1$ and $t(k, \beta^m) \ge \beta - 1$. In particular, this is the case in the following situations:*

(1) *$q > \beta^m \max\left\{2\ell^2 - \ell, \sqrt{12\beta - 47/4} + 3/2\right\}$ and $q - 2\ell\beta^m \ge k \ge 2\ell\beta^m$;*

(2) *$q > \beta^m \max\left\{\ell(\sqrt{6\ell - 23/4} + 3/2), \sqrt{12\beta - 47/4} + 3/2\right\}$ and $q - 3\ell\beta^m \ge k \ge 3\ell\beta^m$.*

Note that this result also applies to $q = 2^\alpha$ and odd k. For example, a simple $(4096, 945, 2832i)$ BIBD exists for any i with $1 \le i \le \binom{4094}{943}/2832$, using $\ell = 9$, $\beta = 35$, and $m = 1$. This case is not covered within the scope of Theorem 2.1.

Theorem 2.4. *Let q be a power p^α of an odd prime, and let $\beta \ge 3$ be odd. Suppose $3 \le k \le q-3$, $p \nmid k$, and $\{c_1, c_2\} = \{1, \ell\beta^m\}$, where $\ell \ge 2$ is even and $m \ge 1$. Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \ell\beta^m) \ge \ell/2-1$ and $t(k, \beta^m) \ge (\beta-1)/2$. In particular, this is the case in the following situations:*

(1) $q > \beta^m \max\left\{\ell^2 - \ell, \sqrt{6\beta - 23/4} + 3/2\right\}$ *and* $q - 2\ell\beta^m \ge k \ge 2\ell\beta^m$;

(2) $q > \beta^m \max\left\{\ell(\sqrt{3\ell - 23/4} + 3/2), \sqrt{6\beta - 23/4} + 3/2\right\}$ *and* $q - 3\ell\beta^m \ge k \ge 3\ell\beta^m$.

For example, a simple $(251, 100, 198i)$ BIBD exists for any i with $1 \le i \le \binom{249}{98}/198$, using $\ell = 2$, $\beta = 5$, and $m = 2$.

Theorem 2.5. *Let q be a power p^α of an odd prime, and let $\ell, \beta \ge 3$ be odd. Suppose $3\ell\beta^m \le k \le q - 3\ell\beta^m$, $p \nmid k$, and $\{c_1, c_2\} = \{2, \ell\beta^m\}$ with $m \ge 1$. Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \ell\beta^m) \ge (\ell-1)/2$ and $t(k, \beta^m) \ge (\beta-1)/2$. In particular, this is the case when $q > \beta^m \max\left\{\ell(\sqrt{3\ell - 11/4} + 3/2), \sqrt{6\beta - 23/4} + 3/2\right\}$.*

For example, a simple $(617, 231, 345i)$ BIBD exists for any i with $1 \le i \le \binom{615}{229}/345$, using $\ell = 7$, $\beta = 11$, and $m = 1$.

Next, we improve the result of Theorem 1.6.

Theorem 2.6. *Let q be a power p^α of an odd prime. Suppose $3 \le k \le q-3$ and $p \nmid k$. Suppose $\{c_1, c_2\} \cap \{1, 2\}$ is not empty, and there is a set D of some proper divisors of c_1c_2 such that*[2]

(1) $\sum_{d \in D} d \ge c_1c_2 - 1$;

(2) *every number i with $1 \le i \le \sum_{d \in D} d$ can be expressed as a sum of distinct elements chosen from D.*

Then the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD.

For example, a simple $(67, 33, 16i)$ BIBD exists for any i with $1 \le i \le \binom{65}{31}/16$. This case is not covered within the scope of Theorem 2.2.

[2] As to which even number n $(= c_1c_2)$ implies a set D with these properties, the reader is referred to the remark after Theorem 14 [6].

Theorem 2.7. *Let q be a power p^α of an odd prime, and let $\beta \geq 3$ be odd. Suppose $\ell\beta^m \leq k \leq q - \ell\beta^m$, $p \nmid k$, and $\{c_1, c_2\} = \{1, \ell\beta^m\}$, where $m \geq 1$ and $\ell \geq 4$ is an even number with the following property: there is a set D of some proper divisors of ℓ such that*

(1) $\sum_{d\in D} d \geq \ell - 1$;

(2) *every number i with $1 \leq i \leq \sum_{d\in D} d$ can be expressed as a sum of distinct elements chosen from D.*

Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \beta^m) \geq (\beta-1)/2$. In particular, this is the case when $q > \beta^m(\sqrt{3(\beta-1)/\delta + 1/4} + 3/2)$, where $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$. More specifically, this is the case when $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$.

For example, a simple $(601, 150, 149i)$ BIBD exists for any i with $1 \leq i \leq \binom{599}{148}/149$, using $\ell = 6$, $\beta = 5$, and $m = 2$.

Theorem 2.8. *Let q be a power p^α of an odd prime, and let $\ell, \beta \geq 3$ be odd. Suppose $\ell\beta^m \leq k \leq q - \ell\beta^m$, $p \nmid k$, and $\{c_1, c_2\} = \{2, \ell\beta^m\}$, where $m \geq 1$ and 2ℓ satisfies the following property: there is a set D of some proper divisors of 2ℓ such that*

(1) $\sum_{d\in D} d \geq 2\ell - 1$;

(2) *every number i with $1 \leq i \leq \sum_{d\in D} d$ can be expressed as a sum of distinct elements chosen from D.*

Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if $t(k, \beta^m) \geq (\beta-1)/2$. In particular, this is the case when $q > \beta^m(\sqrt{3(\beta-1)/\delta + 1/4} + 3/2)$, where $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$. More specifically, this is the case when $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$.

For example, a simple $(9001, 3375, 5061i)$ BIBD exists for any i with $1 \leq i \leq \binom{8999}{3373}/5061$, using $\ell = 9$, $\beta = 5$, and $m = 3$. This illustrates a case which is not covered within the scope of Theorem 2.2.

3. Proofs of Theorem 2.1 to Theorem 2.8

First, we quote some known results, which are used in the proofs. Suppose c divides $q-1$ and Φ is a subgroup of F^* with $|\Phi| = c$.

(1) Let $\mathcal{Z}_1(k, c)$ be the collection of first-type ZSGBs S with block size k and $\Phi \leq \mathrm{Stab}_{F^*}(S)$; let $Z_1(k, c)$ denote the cardinality of $\mathcal{Z}_1(k, c)$. Similarly, let $\mathcal{Z}_2(k, c)$ be

the collection of second-type ZSGBs S with block size k and $\Phi \leq \mathrm{Stab}_{F^*}(S)$; let $Z_2(k,c)$ denote the cardinality of $\mathcal{Z}_2(k,c)$. Let $\mathcal{Z}(k,c) = \mathcal{Z}_1(k,c) \cup \mathcal{Z}_2(k,c)$ and let $Z(k,c)$ denote its cardinality.

(2) Let $N_1(k,c)$ be the number of S in $\mathcal{Z}_1(k,c)$ with $\mathrm{Stab}_{F^*}(S) = \Phi$. Similarly, let $N_2(k,c)$ be the number of S in $\mathcal{Z}_2(k,c)$ with $\mathrm{Stab}_{F^*}(S) = \Phi$. Let $N(k,c)$ be the number of S in $\mathcal{Z}(k,c)$ with $\mathrm{Stab}_{F^*}(S) = \Phi$.

Theorem 3.1. [6, Theorem 9] *Suppose $p \nmid k$, then $t(k,c) = cN(k,c)/(q-1)$, where $N(k,c)$ can be computed by the inclusion-exclusion formula with respect to distinct prime divisors of $\gcd(k,q-1)/c$ or $\gcd(k-1,q-1)/c$ stated in the following.*

(1) *When $c > 1$ and c divides $\gcd(k,q-1)$, let $\gcd(k,q-1)/c = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$ if $\gcd(k,q-1)/c > 1$. Then*

$$N(k,c) = N_1(k,c) = Z_1(k,c) - \sum_i Z_1(k,cp_i) + \sum_{i\neq j} Z_1(k,cp_ip_j) - \cdots .$$

(2) *When $c > 1$ and c divides $\gcd(k-1,q-1)$, let $\gcd(k-1,q-1)/c = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$ if $\gcd(k-1,q-1)/c > 1$. Then*

$$N(k,c) = N_2(k,c) = Z_2(k,c) - \sum_i Z_2(k,cp_i) + \sum_{i\neq j} Z_2(k,cp_ip_j) - \cdots .$$

(3) *When $\gcd(k,q-1) > 1$, let $\gcd(k,q-1) = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$; when $\gcd(k-1,q-1) > 1$, let $\gcd(k-1,q-1) = q_1^{f_1}q_2^{f_2}\cdots q_\ell^{f_\ell}$. Then*

$$N(k,1) = Z(k,1) + \left(-\sum_i Z_1(k,p_i) + \sum_{i\neq j} Z_1(k,p_ip_j) - \cdots\right) + \left(-\sum_i Z_2(k,q_i) + \sum_{i\neq j} Z_2(k,q_iq_j) - \cdots\right).$$

Corollary 3.2. [6, Corollary 2] *Suppose $p \nmid k$, we have the following estimates on $t_1(k,c)$, $t_2(k,c)$, and $t(k,c)$.*

(1) $\left\lceil \frac{c}{q-1}\binom{(q-1)/c}{k/c}\right\rceil \geq t_1(k,c) \geq \frac{c}{q-1}\left(\binom{(q-1)/c}{k/c} - \sum_{\substack{ch\mid\gcd(k,q-1)\\ h \text{ prime}}}\binom{(q-1)/ch}{k/ch}\right)$, *and $t(k,c) = t_1(k,c)$ if c divides $\gcd(k,q-1)$ and $c > 1$.*

(2) $\left\lceil \frac{c}{q-1}\binom{(q-1)/c}{(k-1)/c}\right\rceil \geq t_2(k,c) \geq \frac{c}{q-1}\left(\binom{(q-1)/c}{(k-1)/c} - \sum_{\substack{ch\mid\gcd(k-1,q-1)\\ h \text{ prime}}}\binom{(q-1)/ch}{(k-1)/ch}\right)$, *and $t(k,c) = t_2(k,c)$ if c divides $\gcd(k-1,q-1)$ and $c > 1$.*

(3) $\left\lceil \frac{1}{q-1}\left(\binom{q}{k}/q - y\right)\right\rceil \geq t(k,1)$
$\geq \frac{1}{q-1}\left(\binom{q}{k}/q - \sum_{\substack{h\mid \gcd(k,q-1)\\ h \text{ prime}}} \binom{(q-1)/h}{k/h} - \sum_{\substack{h\mid \gcd(k-1,q-1)\\ h \text{ prime}}} \binom{(q-1)/h}{(k-1)/h}\right)$, *where* $y = 0$ *if* $p = 2$; $y = \binom{(q-1)/2}{k/2}$ *if* $p \neq 2$ *and* k *is even; and* $y = \binom{(q-1)/2}{(k-1)/2}$ *if* $p \neq 2$ *and* k *is odd.*

When (1) $c = \gcd(k, q-1)$ *in the first expression,* (2) $c = \gcd(k-1, q-1)$ *in the second expression, and* (3) $\gcd(k(k-1), q-1) = 1$ *or* 2 *in the third expression, the equalities hold, respectively. When* (1) $\gcd(k, q-1)/c$ *does not have two distinct prime divisors in the first expression,* (2) $\gcd(k-1, q-1)/c$ *does not have two distinct prime divisors in the second expression, and* (3) $\gcd(k, q-1)$ *and* $\gcd(k-1, q-1)$ *do not have two distinct prime divisors in the third expression, the lower bounds are reached, respectively.*

We need two lemmas in the proofs.

Lemma 3.3. *Let* q *be a prime power* p^α. *Suppose* $p \nmid k$, $\beta > 1$, $k > \beta^m$, *and* $\ell\beta^m = \gcd(k, q-1)$ *(or* $\ell\beta^m = \gcd(k-1, q-1)$*). Then,* $t(k,\beta) \geq t(k,\beta^2) \geq \cdots \geq t(k,\beta^m)$.

Proof. We give the proof for $\ell\beta^m = \gcd(k, q-1)$. From Corollary 3.2, we know

$$\left\lceil \frac{\beta^i}{q-1}\binom{(q-1)/\beta^i}{k/\beta^i}\right\rceil \geq t(k,\beta^i) \geq \frac{\beta^i}{q-1}\left\lceil \binom{(q-1)/\beta^i}{k/\beta^i} - \sum_{\substack{h\mid \ell\beta\\ h \text{ prime}}} \binom{(q-1)/\beta^i h}{k/\beta^i h}\right\rceil$$

for $1 \leq i < m$. We point out that the inequality

$$\binom{(q-1)/\beta^i}{k/\beta^i} \geq \beta\binom{(q-1)/\beta^{i+1}}{k/\beta^{i+1}} + \sum_{\substack{h\mid \ell\beta\\ h \text{ prime}}} \binom{(q-1)/\beta^i h}{k/\beta^i h}$$

implies $t(k,\beta^i) \geq \frac{\beta^i}{q-1}\left\lceil \binom{(q-1)/\beta^i}{k/\beta^i} - \sum_{\substack{h\mid \ell\beta\\ h \text{ prime}}} \binom{(q-1)/\beta^i h}{k/\beta^i h}\right\rceil \geq t(k,\beta^{i+1})$. We also need to apply the following inequality: $\binom{(q-1)/ch}{k/ch} \leq \binom{(q-1)/c}{k/c}/h^{k/ch}$. Therefore $t(k,\beta^i) \geq t(k,\beta^{i+1})$ $(1 \leq i < m)$ holds as long as

$$\frac{\beta}{\beta^{\frac{k}{\beta^{i+1}}}} + \sum_{\substack{h\mid \ell\beta\\ h \text{ prime}}} \frac{1}{h^{\frac{k}{\beta^i h}}}$$

is less than or equal to 1. This holds according to the following reasons. Since $k > \beta^m$ and $\beta > 1$, we have

$$\frac{\beta}{\beta^{\frac{k}{\beta^{i+1}}}} \leq \frac{1}{\beta} \leq \frac{1}{2}, \quad 1 \leq i < m.$$

We claim that $\sum_{\substack{h\mid n\\ h \text{ prime}}} 1/h^{n/h} \leq 1/2$ for any number $n \geq 2$. Let $\omega(n)$ denote the number of distinct prime divisors of n, and let $\Omega(n)$ denote the number of prime divisors of n,

counted with multiplicity. Then, $\omega(n) \le \Omega(n) \le \log_2 n$. Let η be the one among the prime divisors of n such that $\eta^{n/\eta}$ is the smallest. It is obvious that $\eta^{n/\eta} \ge 2\log_2 n$. Therefore, $\sum_{\substack{h\mid n\\ h\,\text{prime}}} 1/h^{n/h} \le (\eta^{n/\eta})^{-1}\log_2 n \le 1/2$. Hence we complete the proof. □

Remark 3.4. In fact, Robin [4] obtains the upper bound of $\omega(n)$ for $n \ge 3$:

$$\omega(n) \le 1.3841\frac{\log n}{\log\log n}; \quad \omega(n) \le \frac{\log n}{\log\log n} + 1.45743\frac{\log n}{(\log\log n)^2}.$$

Lemma 3.5. *Let q be a prime power p^α and let $c > 1$. Suppose $p \nmid k$ and $3 \le k \le q-3$. We have the following lower bounds for $t_1(k,c)$ and $t_2(k,c)$.*

(1) $t_1(k,c) \ge \delta\binom{(q-1)/c}{k/c}\frac{c}{q-1}$ *if* $c \mid \gcd(k, q-1)$, *where* $\delta = 1 - \sum_{\substack{h\mid k/c\\ h\,\text{prime}}} (h^{k/ch})^{-1}$.

(2) $t_2(k,c) \ge \delta\binom{(q-1)/c}{(k-1)/c}\frac{c}{q-1}$ *if* $c \mid \gcd(k-1, q-1)$, *where* $\delta = 1 - \sum_{\substack{h\mid (k-1)/c\\ h\,\text{prime}}} (h^{(k-1)/ch})^{-1}$.

In particular, when $q > \xi c + 1$, we have the following lower bounds in these situations.

(1) $t(k,c) > (\xi-1)/4$ *if* $q - 2c \ge k \ge 2c$;

(2) $t(k,c) > (\xi-1)(\xi-2)/12$ *if* $q - 3c \ge k \ge 3c$.

Proof. We here give the proof for $c \mid \gcd(k, q-1)$, $q > \xi c + 1$, and $q - 3c \ge k \ge 3c$. From Corollary 3.2 we have

$$\begin{aligned}
t(k,c) = t_1(k,c) &\ge \frac{c}{q-1}\left(\binom{(q-1)/c}{k/c} - \sum_{\substack{ch\mid \gcd(k,q-1)\\ h\,\text{prime}}} \binom{(q-1)/ch}{k/ch}\right)\\
&\ge \frac{c}{q-1}\left(\binom{(q-1)/c}{k/c} - \sum_{\substack{ch\mid \gcd(k,q-1)\\ h\,\text{prime}}} \binom{(q-1)/c}{k/c}(h^{\frac{k}{ch}})^{-1}\right)\\
&\ge \frac{c}{q-1}\binom{(q-1)/c}{k/c}\left(1 - \sum_{\substack{h\mid \frac{k}{c}\\ h\,\text{prime}}} (h^{\frac{k}{ch}})^{-1}\right)\\
&= \delta\binom{(q-1)/c}{k/c}\frac{c}{q-1} \ge \frac{1}{2}\binom{(q-1)/c}{3}\frac{c}{q-1}\\
&= \frac{1}{2}\cdot\frac{1}{6}\left(\frac{q-1}{c} - 1\right)\left(\frac{q-1}{c} - 2\right) > \frac{1}{12}(\xi-1)(\xi-2).
\end{aligned}$$

□

Now, we give the proofs of Theorems 2.1–2.8.

Proof of Theorem 2.1. Notice that $\lambda_{\min} = k(k-1)/\beta^m$. We here sketch the proof for $c_1 = \beta^m$ and $c_2 = 1$. Without loss of generality, we assume that $k < q/2 = 2^{(\alpha-1)}$. We have $t(k, \beta^m) = t_1(k, \beta^m) = \binom{(q-1)/\beta^m}{k/\beta^m}\beta^m/(q-1)$. Now, we are going to find a list Γ with the properties: (1) $\sum_{\tau\in\Gamma}\tau = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $1 \le j \le \beta^m - 1$ can be expressed as a sum of numbers chosen from Γ. By the assumption on the value of $t(k, \beta^m)$ and the fact $t(k, \beta) \ge t(k, \beta^2) \ge \cdots \ge t(k, \beta^m)$, we have $\beta - 1$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \le i \le m-1$. So we put $\beta - 1$ copies of $\beta^i\lambda_{\min}$ into Γ for each i with $0 \le i \le m-1$. The numbers in Γ can represent the following numbers: $j\lambda_{\min}$ for $1 \le j \le \beta^m - 1$. Hence Γ meets the requirements of Theorem 1.5. The particular case are derived for the following situation: $q - 3\beta^m \ge k \ge 3\beta^m$ and $t(k, \beta^m) \ge \binom{(q-1)/\beta^m}{3}\beta^m/(q-1) \ge \beta - 1$. □

Proof of Theorem 2.2. We have $\lambda_{\min} = k(k-1)/(6\beta^m)$ and β is odd. The idea of the proof is in essential on finding a sublist Γ mentioned in Theorem 1.5. We here give the proof for $c_1 = 3\beta^m$ and $c_2 = 2$. We assume that $k \le (q-1)/2$. First we have $t(k, \beta^m) = t_1(k, \beta^m) = \left(\binom{(q-1)/\beta^m}{k/\beta^m} - \binom{(q-1)/3\beta^m}{k/3\beta^m}\right)\beta^m/(q-1)$ from Theorem 3.1. We are going to find a list Γ with the following properties: (1) $\sum_{\tau\in\Gamma}\tau = (6\beta^m - 1)\lambda_{\min} = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $1 \le j \le 6\beta^m - 1$ can be expressed as a sum of numbers chosen from Γ. Let us collect the following numbers to form the sublist Γ.

(1) Since $t(k, 3\beta^m) \ge 1$ we have a simple $(q, k, 2\lambda_{\min})$ BIBD from the affine construction; this BIBD can be partitioned into two isomorphic BIBDs. Thus we put two copies of $\lambda_{\min}$ into Γ.

(2) By the assumption on the value of $t(k, \beta^m)$ and the fact $t(k, \beta) \ge t(k, \beta^2) \ge \cdots \ge t(k, \beta^m)$ from Lemma 3.3, we have $(\beta - 1)/2$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \le i \le m-1$; moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. So we can put $\beta - 1$ copies of $3\beta^i\lambda_{\min}$ into Γ for each i with $0 \le i \le m-1$.

(3) We further put one copy of $3\beta^m\lambda_{\min}$ into Γ by the fact that $t(k, 1) \ge 1$ and such BIBD can be partitioned into two isomorphic BIBDs.

The resulting Γ then satisfies the specified conditions. Hence Γ meets the requirements of Theorem 1.5 and we finish this part of the proof.

Now we derive the results for the particular situations.

(1) When $k = 3\beta^m$, $3\beta^m + 1$, $q - 3\beta^m$, or $q - 3\beta^m - 1$, we require that $t(k, \beta^m) = \left(\binom{(q-1)/\beta^m}{3} - \binom{(q-1)/3\beta^m}{1}\right)\beta^m/(q-1) \ge (\beta-1)/2$. From this we obtain

$$q > \beta^m(\sqrt{3\beta - 3/4} + 3/2).$$

(2) When $q - 9\beta^m \geq k \geq 9\beta^m$, let us consider the case when $t(k, \beta^m) = t_1(k, \beta^m)$.

$$\begin{aligned} t(k,\beta^m) &= \frac{\beta^m}{q-1}\left[\binom{(q-1)/\beta^m}{k/\beta^m} - \binom{(q-1)/3\beta^m}{k/3\beta^m}\right] \\ &\geq \frac{\beta^m}{q-1}\left(1 - \frac{1}{3^{k/3\beta^m}}\right)\binom{(q-1)/\beta^m}{k/\beta^m} \geq \frac{\beta^m}{q-1}\left(1-\frac{1}{3^2}\right)\binom{(q-1)/\beta^m}{4} \\ &= \frac{2}{9}\left(\frac{q-1}{\beta^m} - 3\right)\frac{\beta^m}{q-1}\binom{(q-1)/\beta^m}{3} \geq \frac{\beta^m}{q-1}\binom{(q-1)/\beta^m}{3}. \end{aligned}$$

Therefore, when $q > \beta^m(\sqrt{3\beta - 11/4} + 3/2)$, the requirement $t(k, \beta^m) \geq (\beta - 1)/2$ is satisfied. □

Proof of Theorem 2.3. Notice that $\lambda_{\min} = k(k-1)/\ell\beta^m$. We here give the proof for $c_1 = \ell\beta^m$ and $c_2 = 1$. We assume that $k \leq [(q-1)/2]$.

We have $t(k, \beta^m) = t_1(k, \beta^m) \geq \left(\binom{(q-1)/\beta^m}{k/\beta^m} - \sum_{\substack{h|\ell \\ h \text{ prime}}} \binom{(q-1)/\beta^m h}{k/\beta^m h}\right)\beta^m/(q-1)$ from Corollary 3.2. We are going to find a list Γ with the following properties: (1) $\sum_{\tau\in\Gamma}\tau \geq (\ell\beta^m - 1)\lambda_{\min} = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $\lambda_{\min} \leq j\lambda_{\min} \leq \sum_{\tau\in\Gamma}\tau$ can be expressed as a sum of numbers chosen from Γ. Let us collect the following numbers to form the sublist Γ.

(1) Since $t(k, \ell\beta^m) \geq \ell - 1$ we have $\ell - 1$ disjoint simple $(q, k, \lambda_{\min})$ BIBDs from the affine constructions. Thus we put $\ell - 1$ copies of $\lambda_{\min}$ into Γ.

(2) By the assumption on the value of $t(k, \beta^m)$ and the fact $t(k, \beta) \geq t(k, \beta^2) \geq \cdots \geq t(k, \beta^m)$, we have $\beta - 1$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \leq i \leq m-1$. So we can put $\beta - 1$ copies of $\ell\beta^i\lambda_{\min}$ into Γ for each i with $0 \leq i \leq m-1$.

The resulting Γ then satisfies the specified conditions. Therefore, Γ meets the requirements of Theorem 1.5. The particular situations are derived as follows.

(1) When $q - 2\ell\beta^m \geq k \geq 2\ell\beta^m$, we require the following two conditions.
Condition 1:

$$t(k, \ell\beta^m) \geq \binom{(q-1)/\ell\beta^m}{2}\frac{\ell\beta^m}{q-1} \geq \ell - 1.$$

This holds when $q > \beta^m(2\ell^2 - \ell)$.

Condition 2:

$$\begin{aligned} t(k,\beta^m) &\geq \left[\binom{(q-1)/\beta^m}{k/\beta^m} - \sum_{\substack{h|\ell \\ h \text{ prime}}} \binom{(q-1)/\beta^m h}{k/\beta^m h}\right]\frac{\beta^m}{q-1} \\ &\geq \delta\binom{(q-1)/\beta^m}{k/\beta^m}\frac{\beta^m}{q-1} \geq \delta\binom{(q-1)/\beta^m}{3}\frac{\beta^m}{q-1} \geq \beta - 1. \end{aligned}$$

Note that $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1} \geq 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{\ell/h})^{-1} \geq 1/2$. This holds when $q > \beta^m(\sqrt{12\beta - 47/4} + 3/2)$.

(2) When $q - 3\ell\beta^m \geq k \geq 3\ell\beta^m$, we use the following similar conditions:

$$t(k, \ell\beta^m) \geq \binom{(q-1)/\ell\beta^m}{3} \frac{\ell\beta^m}{q-1} \geq \ell - 1,$$
$$t(k, \beta^m) \geq \delta \binom{(q-1)/\beta^m}{3} \frac{\beta^m}{q-1} \geq \beta - 1.$$

These hold when $q > \beta^m \max\left\{\ell(\sqrt{6\ell - 23/4} + 3/2), \sqrt{12\beta - 47/4} + 3/2\right\}$. □

Proof of Theorem 2.4. The proof is similar to that of Theorem 2.3. The different part is on collecting the following numbers to form the sublist Γ.

(1) Since $t(k, \ell\beta^m) \geq \ell/2 - 1$ we have $\ell/2 - 1$ disjoint simple $(q, k, \lambda_{\min})$ BIBDs from the affine constructions. Thus we put $\ell/2 - 1$ copies of $\lambda_{\min}$ into Γ.

(2) We have $(\beta - 1)/2$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \leq i \leq m - 1$; moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. So we can put $\beta - 1$ copies of $\frac{1}{2}\ell\beta^i\lambda_{\min}$ into Γ for each i with $0 \leq i \leq m - 1$.

(3) We further put one copy of $\frac{1}{2}\ell\beta^m\lambda_{\min}$ into Γ by the fact that $t(k, 1) \geq 1$ and such BIBD can be partitioned into two isomorphic BIBDs.

The particular situations are derived as follows.

(1) When $q - 2\ell\beta^m \geq k \geq 2\ell\beta^m$, we require the following two conditions:

$$t(k, \ell\beta^m) \geq \binom{(q-1)/\ell\beta^m}{2} \frac{\ell\beta^m}{q-1} \geq \frac{\ell}{2} - 1,$$
$$t(k, \beta^m) \geq \left[\binom{(q-1)/\beta^m}{k/\beta^m} - \sum_{\substack{h|\ell \\ h \text{ prime}}} \binom{(q-1)/\beta^m h}{k/\beta^m h} \right] \frac{\beta^m}{q-1}$$
$$\geq \delta \binom{(q-1)/\beta^m}{k/\beta^m} \frac{\beta^m}{q-1} \geq \frac{1}{2} \binom{(q-1)/\beta^m}{3} \frac{\beta^m}{q-1} \geq \frac{\beta - 1}{2},$$

where $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1} \geq 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{\ell/h})^{-1} \geq 1/2$.

(2) When $q - 3\ell\beta^m \geq k \geq 3\ell\beta^m$, we use the following similar conditions:

$$t(k, \ell\beta^m) \geq \binom{(q-1)/\ell\beta^m}{3} \frac{\ell\beta^m}{q-1} \geq \frac{\ell}{2} - 1,$$
$$t(k, \beta^m) \geq \frac{1}{2} \binom{(q-1)/\beta^m}{3} \frac{\beta^m}{q-1} \geq \frac{\beta - 1}{2}.$$

□

Proof of Theorem 2.5. Notice that $\lambda_{\min} = k(k-1)/(2\ell\beta^m)$. We here give the proof for $c_1 = \ell\beta^m$ and $c_2 = 2$. We are going to find a list Γ with the following properties: (1) $\sum_{\tau\in\Gamma}\tau \geq (2\ell\beta^m - 1)\lambda_{\min} = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $\lambda_{\min} \leq j\lambda_{\min} \leq \sum_{\tau\in\Gamma}\tau$ can be expressed as a sum of numbers chosen from Γ. Let us collect the following numbers to form the sublist Γ.

(1) Since $t(k, \ell\beta^m) \geq (\ell-1)/2$ we have $(\ell-1)/2$ disjoint simple $(q, k, 2\lambda_{\min})$ BIBDs from the affine constructions. Moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. Thus we put $\ell - 1$ copies of $\lambda_{\min}$ into Γ.

(2) We have $(\beta-1)/2$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \leq i \leq m-1$; moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. So we can put $\beta - 1$ copies of $\ell\beta^i\lambda_{\min}$ into Γ for each i with $0 \leq i \leq m-1$.

(3) We further put one copy of $\ell\beta^m\lambda_{\min}$ into Γ by the fact that $t(k, 1) \geq 1$ and such BIBD can be partitioned into two isomorphic BIBDs.

The resulting Γ then satisfies the specified conditions. Therefore, Γ meets the requirements of Theorem 1.5.

We require the following conditions for the particular case:

$$t(k, \ell\beta^m) \geq \binom{(q-1)/\ell\beta^m}{3}\frac{\ell\beta^m}{q-1} \geq \frac{\ell-1}{2},$$
$$t(k, \beta^m) \geq \frac{1}{2}\binom{(q-1)/\beta^m}{3}\frac{\beta^m}{q-1} \geq \frac{\beta-1}{2}.$$

□

Proof of Theorem 2.6. This improvement to Theorem 1.6 is made for the situation when $\{c_1, c_2\} = \{2, d_1\}$ with odd $d_1 > 1$. We assume that $k \leq (q-1)/2$.

When $q - 3d_1 \geq k \geq 3d_1$, we need $t(k, d_1/d) \geq 2$ whenever d is a proper divisor of d_1. According to Lemma 3.5, it suffices to show that $q > 5(d_1/d) + 1$. Since $q > 2k \geq 6d_1 > 5(d_1/d) + 1$ it is clearly true. This part then follows.

When $k = d_1$ (or $k = d_1 + 1$), we still have $t(k, d_1/d) \geq 2$ for any proper divisor d of d_1 with $d \neq 1$, since $q > 2k \geq 2d_1 = (2d)(d_1/d) > 5(d_1/d) + 1$. Therefore, the problem appears at $d = 1$, i.e., we can only have $t(k, d_1) = 1$. Thus, we can not put $\lambda_{\min}$ and $2\lambda_{\min}$ into the list Γ at the same time.

We are going to make some adjustments in order to get a suitable list Γ. Note that it is easy to see that $3 \mid d_1$, since $4 \notin D$ and $4 = 1 + 3$ is the unique expressed sum of 4 by distinct numbers. Therefore, we obtain $1, 2, 3 \in D$. We now make a list $L = (1, 1, 3, 3, \ldots)$ where the rest part of L are exactly the elements of $D \setminus \{1, 2, 3\}$—if there is any. We claim that this list L has the properties:

(1) $\sum_{d\in L} d = \left(\sum_{d\in D} d\right) + 2 \geq c_1c_2 + 1$;

(2) every number i with $1 \le i \le \sum_{d\in L} d$ can be expressed as a sum of numbers chosen from L.

Let i be expressed, in expression E_1, as a sum of distinct elements chosen from D. We express i, in expression E_2, as a sum of numbers chosen from L in the following.

(1) If 2 is not used in E_1, then E_2 is the same as E_1.

(2) If 2 is used and 1 is not used in E_1, then E_2 is formed by removing 2 and adding two 1 in E_1.

(3) If 2 and 1 are used in E_1, no matter 3 is used or not, then E_2 is formed by removing $1, 2$ and adding one 3 in E_1.

Also note that the expression for the number $i = \left(\sum_{d\in D} d\right) + 1 = \left(\sum_{d\in L} d\right) - 1$ is formed by removing 1 from the sum $\sum_{d\in L} d$. One can see that the two 1 and two 3 in L correspond to BIBDs with parameters $(q, k, 2\lambda_{\min})$ and $(q, k, 6\lambda_{\min})$[3], respectively; each BIBD can be partitioned into two isomorphic BIBDs. The list Γ is then formed by putting one copy of $d\lambda_{\min}$ into Γ for each number d in the list L. Hence Γ meets the requirements in Theorem 1.5 and we complete the proof. □

Proof of Theorem 2.7. Notice that $\lambda_{\min} = k(k-1)/\ell\beta^m$. We here give the proof for $c_1 = \ell\beta^m$ and $c_2 = 1$. We assume that $k \le (q-1)/2$.

We have $t(k, \beta^m) = t_1(k, \beta^m) \ge \left(\binom{(q-1)/\beta^m}{k/\beta^m} - \sum_{\substack{h|\ell \\ h \text{ prime}}} \binom{(q-1)/\beta^m h}{k/\beta^m h} \right) \beta^m/(q-1)$ from Corollary 3.2. We are going to find a list Γ with the following properties: (1) $\sum_{\tau\in\Gamma} \tau \ge (\ell\beta^m - 1)\lambda_{\min} = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $\lambda_{\min} \le j\lambda_{\min} \le \sum_{\tau\in\Gamma} \tau$ can be expressed as a sum of numbers chosen from Γ. Let us collect the following numbers to form the sublist Γ.

(1) For each $d \in D$, we have a simple $(q, k, d\lambda_{\min})$ BIBD from the affine construction, since $t(k, (\ell/d)\beta^m) \ge 1$. Then, a simple $(q, k, i\lambda_{\min})$ BIBD exists for any i with $1 \le i \le \sum_{d\in D} d$, by collecting the BIBDs corresponding to the distinct numbers selected from D in the expressed sum for i. Thus we put one copy of $d\lambda_{\min}$ into Γ for $d \in D$.

(2) By the assumption on the value of $t(k, \beta^m)$ and the fact $t(k, \beta) \ge t(k, \beta^2) \ge \cdots \ge t(k, \beta^m)$, we have $(\beta-1)/2$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \le i \le m-1$; moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. So we can put $\beta - 1$ copies of $\frac{1}{2}\ell\beta^i\lambda_{\min}$ into Γ for each i with $0 \le i \le m-1$.

[3]This argument does not apply to $q = 7$ and $k = 3$, since there is no simple $(7, 3, 6)$ BIBD.

(3) We further put one copy of $\frac{1}{2}\ell\beta^m\lambda_{\min}$ into Γ by the fact that $t(k,1) \geq 1$ and such BIBD can be partitioned into two isomorphic BIBDs.

The resulting Γ then satisfies the specified conditions. Therefore, Γ meets the requirements of Theorem 1.5.

The particular case is derived by requiring

$$t(k,\beta^m) \geq \left[\binom{(q-1)/\beta^m}{k/\beta^m} - \sum_{\substack{h|\ell \\ h \text{ prime}}} \binom{(q-1)/\beta^m h}{k/\beta^m h} \right] \frac{\beta^m}{q-1}$$
$$\geq \delta \binom{(q-1)/\beta^m}{k/\beta^m} \frac{\beta^m}{q-1} \geq \delta \binom{(q-1)/\beta^m}{3} \frac{\beta^m}{q-1} \geq \frac{\beta-1}{2}.$$

Therefore, we have $\beta^m(\sqrt{6\beta - 23/4} + 3/2) \geq \beta^m(\sqrt{3(\beta-1)/\delta + 1/4} + 3/2)$. Note that $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1} \geq 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{\ell/h})^{-1} \geq 1/2$. Hence, we can require that $\binom{(q-1)/\beta^m}{3} \frac{\beta^m}{q-1} \geq \beta - 1$ for the special case. □

Proof of Theorem 2.8. Notice that $\lambda_{\min} = k(k-1)/(2\ell\beta^m)$. We here give the proof for $c_1 = \ell\beta^m$ and $c_2 = 2$. We assume that $k \leq (q-1)/2$.

We are going to find a list Γ with the following properties: (1) $\sum_{\tau\in\Gamma} \tau \geq (2\ell\beta^m - 1)\lambda_{\min} = k(k-1) - \lambda_{\min}$; (2) any $j\lambda_{\min}$ with $\lambda_{\min} \leq j\lambda_{\min} \leq \sum_{\tau\in\Gamma} \tau$ can be expressed as a sum of numbers chosen from Γ. Let us collect the following numbers to form the sublist Γ.

(1) For each $d \in D$, we make the discussion according to the parity of d.

   (a) When d is odd, we have a simple $(q, k, 2d\lambda_{\min})$ BIBD in the affine constructions, since $t(k, (\ell/d)\beta^m) \geq 1$; this BIBD can be partitioned into two isomorphic BIBDs. At this time we put one copy of $d\lambda_{\min}$ into Γ.

   (b) When d is even, we have a simple $(q, k, d\lambda_{\min})$ BIBD from the affine construction, since $t(k, (2\ell/d)\beta^m) \geq 1$. Therefore, we can put one copy of $d\lambda_{\min}$ into Γ.

   Note that for any odd $d \in D$ such that $2d$ is also in D, in order to have two disjoint simple BIBDs, we need $t(k, (\ell/d)\beta^m) \geq 2$. According to Lemma 3.5, this happens when $q > 5(\ell/d)\beta^m + 1$. It is clearly true when $q - 3\ell\beta^m \geq k \geq 3\ell\beta^m$, since $q > 2k \geq 6\ell\beta^m$. So we can put one copy of $d\lambda_{\min}$ into Γ for each $d \in D$. Then, a simple $(q, k, i\lambda_{\min})$ BIBD exists for any i with $1 \leq i \leq \sum_{d\in D} d$, by collecting the BIBDs corresponding to the distinct numbers selected from D in the expressed sum for i.

When $k = \ell\beta^m$ (or $k = \ell\beta^m+1$), we still have $t(k, (\ell/d)\beta^m) \geq 2$ for any proper divisor d of ℓ with $d \neq 1$, since $q > 2k \geq 2\ell\beta^m = (2d)(\ell/d)\beta^m \geq 6(\ell/d)\beta^m$. Therefore, the problem appears at $d = 1$, i.e., we can only have $t(k, \ell\beta^m) = 1$. Thus, we can not put $\lambda_{\min}$ and $2\lambda_{\min}$ into the list Γ at the same time. Note that we have $1, 2, 3 \in D$. The discussion is then similar to the late part of the proof of Theorem 2.6. So we make a list $L = (1, 1, 3, 3, \ldots)$ where the rest part of L are exactly the elements of $D \setminus \{1, 2, 3\}$—if there is any. We claim that this list L has the properties:

(a) $\sum_{d\in L} d = \left(\sum_{d\in D} d\right) + 2 \geq 2\ell + 1$;

(b) every number i with $1 \leq i \leq \sum_{d\in L} d$ can be expressed as a sum of numbers chosen from L.

So we can put one copy of $d\lambda_{\min}$ into Γ for each $d \in L$. Then, a simple $(q, k, i\lambda_{\min})$ BIBD exists for any i with $1 \leq i \leq \sum_{d\in L} d$, by collecting the BIBDs corresponding to the numbers selected from L in the expressed sum for i.

(2) We claim that $t(k, \beta^m) \geq (\beta - 1)/2$ when $q > \beta^m(\sqrt{3(\beta - 1)/\delta + 1/4} + 3/2)$, where $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$. This part of proof is exactly the same as that for Theorem 2.7. Then, by the fact $t(k, \beta) \geq t(k, \beta^2) \geq \cdots \geq t(k, \beta^m)$, we have $(\beta-1)/2$ disjoint simple $(q, k, \beta^i k(k-1)/\beta^m)$ BIBDs for each i with $0 \leq i \leq m-1$; moreover, each of these BIBDs can be partitioned into two isomorphic BIBDs. So we can put $\beta - 1$ copies of $\ell\beta^i\lambda_{\min}$ into Γ for each i with $0 \leq i \leq m - 1$.

(3) We further put one copy of $\ell\beta^m\lambda_{\min}$ into Γ by the fact that $t(k, 1) \geq 1$ and such BIBD can be partitioned into two isomorphic BIBDs.

The resulting Γ then satisfies the specified conditions. Therefore, Γ meets the requirements of Theorem 1.5. □

4. Conclusions and remarks

We give more results showing that, when the number of elements is a prime power, in many situations the necessary conditions are also sufficient for the existence of a simple BIBD.

We summarize the particular results as follows. Let $q = p^\alpha$, $p \neq 2$, $3 \leq k \leq q - 3$ with $p \nmid k$, $c_1 = \gcd(k, q - 1)$, and $c_2 = \gcd(k - 1, q - 1)$. Then, all simple BIBDs whose parameters (q, k, λ) satisfy the necessary conditions exist in the following situations.

(1) $\{c_1, c_2\} = \{2, 3\beta^m\}$ with odd $\beta \geq 3$, $q > \beta^m(\sqrt{3\beta - 11/4} + 3/2)$, and $q - 9\beta^m \geq k \geq 9\beta^m$.

(2) $\{c_1, c_2\} = \{1, \ell\beta^m\}$ with $\ell, \beta \geq 2$, $q > \beta^m \max\left\{2\ell^2 - \ell, \sqrt{12\beta - 47/4} + 3/2\right\}$, and $q - 2\ell\beta^m \geq k \geq 2\ell\beta^m$.

(3) $\{c_1, c_2\} = \{1, \ell\beta^m\}$ with even $\ell \geq 2$ and odd $\beta \geq 3$, $q > \beta^m \max\{\ell^2 - \ell, \sqrt{6\beta - 23/4} + 3/2\}$, and $q - 2\ell\beta^m \geq k \geq 2\ell\beta^m$.

(4) $\{c_1, c_2\} = \{2, \ell\beta^m\}$ with odd $\ell, \beta \geq 3$, $q > \beta^m \max\{\ell(\sqrt{3\ell - 11/4}+3/2), \sqrt{6\beta - 23/4} + 3/2\}$, and $q - 3\ell\beta^m \geq k \geq 3\ell\beta^m$.

(5) $\{c_1, c_2\} \cap \{1, 2\}$ is not empty, and there is a set D of some proper divisors of c_1c_2 such that (a) $\sum_{d\in D} d \geq c_1c_2 - 1$; (b) every number i with $1 \leq i \leq \sum_{d\in D} d$ can be expressed as a sum of distinct elements chosen from D.

(6) $\{c_1, c_2\} = \{1, \ell\beta^m\}$ with odd $\beta \geq 3$, $q > \beta^m(\sqrt{6\beta - 23/4}+3/2)$, $q-\ell\beta^m \geq k \geq \ell\beta^m$, and there is a set D of some proper divisors of the even number $\ell \geq 4$ such that (a) $\sum_{d\in D} d \geq \ell - 1$; (b) every number i with $1 \leq i \leq \sum_{d\in D} d$ can be expressed as a sum of distinct elements chosen from D.

(7) $\{c_1, c_2\} = \{2, \ell\beta^m\}$ with odd $\ell, \beta \geq 3$, $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$, $q - \ell\beta^m \geq k \geq \ell\beta^m$, and there is a set D of some proper divisors of 2ℓ such that (a) $\sum_{d\in D} d \geq 2\ell-1$; (b) every number i with $1 \leq i \leq \sum_{d\in D} d$ can be expressed as a sum of distinct elements chosen from D.

We also obtain particular results for $q = 2^\alpha$. Suppose $3 \leq k \leq q - 3$ is odd; let $c_1 = \gcd(k, q - 1)$ and $c_2 = \gcd(k - 1, q - 1)$. Then, all simple BIBDs whose parameters $(q = 2^\alpha, k, \lambda)$ satisfy the necessary conditions exist in the following situations.

(1) $\{c_1, c_2\} = \{1, \beta^m\}$ with odd $\beta \geq 3$, $q - 3\beta^m \geq k \geq 3\beta^m$, and $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$.

(2) $\{c_1, c_2\} = \{1, \ell\beta^m\}$ with odd $\ell, \beta \geq 3$, $q - 3\ell\beta^m \geq k \geq 3\ell\beta^m$, and $q > \beta^m \max\left\{\ell(\sqrt{6\ell - 23/4} + 3/2), \sqrt{12\beta - 47/4} + 3/2\right\}$.

Note that when ℓ, β, and m are specified in the above various situations, there are only a finite number of unknown cases left, whose values q are below the valid bounds. Thus, in order to reduce the amount of the remaining unknown cases, it is reasonable to make the lower bounds as small as possible.

We are informed by a referee that Dehon in 1983 proved the following theorem: There exists a simple $(v, 3, \lambda)$ BIBD if and only if $\lambda \leq v-2$, $\lambda v(v-1) \equiv 0 \mod 6$, and $\lambda(v-1) \equiv 0 \mod 2$ [3].

Acknowledgments

The author thanks the referees for reading this article, for correcting the errors, and for making suggestions. This research is supported in part by the Taiwan (R.O.C.) Ministry of Science and Technology Grant MOST103-2115-M-024-002.

References

[1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Second ed., Cambridge University Press, Cambridge, 1999. http://dx.doi.org/10.1017/cbo9780511549533

[2] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, Second ed., CRC Press, Boca Raton, 2007.

[3] M. Dehon, *On the existence of* 2*-designs* $S_\lambda(2,3,v)$ *without repeated blocks*, Discrete Math. **43** (1983), no. 2-3, 155–171. http://dx.doi.org/10.1016/0012-365x(83)90153-x

[4] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. **42** (1983), no. 4, 367–389.

[5] H.-M. Sun, *From planar nearrings to generating blocks*, Taiwanese J. Math. **14** (2010), no. 5, 1713–1739. http://journal.tms.org.tw/index.php/TJM/article/view/276

[6] ———, *On the existence of simple BIBDs with number of elements a prime power*, J. Combin. Des. **21** (2013), no. 2, 47–59. http://dx.doi.org/10.1002/jcd.21309

[7] ———, Correction to: *On the existence of simple BIBDs with number of elements a prime power*, J. Combin. Des. **21** (2013), no. 10, 478–479. http://dx.doi.org/10.1002/jcd.21360

[8] R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory **4** (1972), no. 1, 17–47. http://dx.doi.org/10.1016/0022-314x(72)90009-1

Hsin-Min Sun
Department of Applied Mathematics, National University of Tainan, Tainan 70005, Taiwan
E-mail address: sunhm@mail.nutn.edu.tw