Super-simple $(v, 5, 4)$ Designs*

Kejun Chen and Ruizhong Wei

Department of Computer Science, Lakehead University

Thunder Bay, ON, P7B 5E1 Canada

Email: kchen3@lakeheadu.ca, wei@ccc.cs.lakeheadu.ca

Abstract

Super-simple designs are useful in constructing codes and designs such as superimposed codes and perfect hash families. Recently, Gronau et al determined the existence of super-simple $(v, 5, 2)$-BIBDs with possible exceptions of $v \in \{75, 95, 115, 135, 195, 215, 231, 285, 365, 385, 515\}$. In this article, we investigate the existence of a super-simple $(v, 5, 4)$-BIBD and show that such a design exists if and only if $v \equiv 0, 1 \pmod 5$ and $v \geq 15$. In addition, we also constructed a super-simple $(v, 5, 2)$-BIBD for $v = 75, 95$, or 385.

Keywords: super-simple designs, group divisible designs, superimposed codes

1 Introduction

A *group divisible design* (or GDD) is a triple $(X, \mathcal{G}, \mathcal{B})$ which satisfies the following properties:

1. $\mathcal{G}$ is a partition of a set X (of *points*) into subsets called *groups*;

2. $\mathcal{B}$ is a set of subsets of X (called *blocks*) such that a group and a block contain at most one common point;

3. Every pair of points from distinct groups occurs in exactly λ blocks.

The *group type* (or *type*) of GDD is the multiset $\{|G| : G \in \mathcal{G}\}$. We shall use an "exponential" notation to describe types: so type $g_1^{u_1} \cdots g_k^{u_k}$ denotes u_i occurrences of g_i, $1 \leq i \leq k$, in the multiset. A GDD with block sizes from a set of positive integers K is called a

*Research supported by NSERC grant 239135-01

(K, λ)-GDD. When $K = \{k\}$, we simply write k for K. When $\lambda = 1$, we simply write K-GDD. A (k, λ)-GDD with group type 1^v is called a *balanced incomplete block design*, denoted by (v, k, λ)-BIBD.

A (K, λ)-GDD, $(X, \mathcal{G}, \mathcal{B})$, is called *resolvable* if its block set $\mathcal{B}$ admits a partition into parallel classes, each parallel class being a partition of the point set X. We denote it by (K, λ)-RGDD.

A design is said to be *simple* if it contains no repeated blocks. A design is said to be *super-simple* if the intersection of any two blocks has at most two elements. When $k = 3$, a super-simple design is just a simple design. When $\lambda = 1$, the designs are always super-simple. In this paper, when we talk about super-simple BIBDs, we usually mean the case that $k \geq 4$ and $\lambda > 1$.

Super-simple designs were introduced by Gronau and Mullin in [10]. The existence of super-simple designs is an interesting extremal problem by itself, but there are also useful applications. For examples, such designs are used in constructing perfect hash families [14] and coverings [4], in the construction of new designs [3] and in the construction of superimposed codes [13]. In statistical planning of experiments, super-simple designs are the ones providing samples with maximum intersection as small as possible.

It is well known that the followings are the necessary conditions for the existence of a super-simple (v, k, λ)-BIBD:

1. $v \geq (k-2)\lambda + 2$;
2. $\lambda(v-1) \equiv 0 \pmod{k-1}$;
3. $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

For the existence of super-simple $(v, 4, \lambda)$-BIBDs, the necessary conditions are known to be sufficient for $\lambda = 2, 3, 4$. Gronau and Mullin solved the case for $\lambda = 2$ in [10], and an alternative proof appeared in [12]. The case of $\lambda = 3$ was solved independently by Khodkar [12] and Chen [6]. The case of $\lambda = 4$ was solved independently by Adams et al. [2] and Chen [7]. The case of $\lambda = 6$ was solved by Chen, Cao and Wei [8]. A recent survey on super-simple $(v, 4, \lambda)$-BIBDs with $v \leq 32$ can be found in [5]. We summarize these known results in the following theorem.

Theorem 1.1 ([10], [12], [6], [2], [7], [8]) *A super-simple $(v, 4, \lambda)$-BIBD exists for $\lambda = 2, 3, 4, 6$ if and only if the following conditions are satisfied:*

1. $\lambda = 2,\ v \equiv 1 \pmod 3$ *and* $v \geq 7$;

2. $\lambda = 3,\ v \equiv 0, 1 \pmod 4$ *and* $v \geq 8$;

3. $\lambda = 4,\ v \equiv 1 \pmod 3$ *and* $v \geq 10$;

4. $\lambda = 6,\ v \geq 14$.

Recently, Gronau et al [11] solved the case of $k = 5$ and $\lambda = 2$. They showed the following.

Theorem 1.2 *A super-simple* $(v, 5, 2)$*-BIBD exists if and only if* $v \equiv 1, 5 \pmod{10}$, $v \neq 5, 15$, *except possibly when* $v \in \{75, 95, 115, 135, 195, 215, 231, 285, 365, 385, 515\}$.

In this article we investigate the existence of super-simple $(v, 5, 4)$-BIBDs. When $k = 5$ and $\lambda = 4$ the necessary condition becomes $v \equiv 0, 1 \pmod 5$ and $v \geq 15$. We shall use direct and recursive constructions to show that this necessary condition is also sufficient. Specifically, we shall prove the following.

Theorem 1.3 *A super-simple* $(v, 5, 4)$*-BIBD exists if and only if* $v \equiv 0, 1 \pmod 5$ *and* $v \geq 15$.

Some recursive constructions used in this paper are listed in Section 2. Section 3 gives direct constructions which are based on a computer search. The proof of Theorem 1.3 will be given in Section 4. In Section 5, for each $v \in \{75, 95, 385\}$, a super-simple $(v, 5, 2)$-BIBD will be constructed. In addition, as an application, a bound of superimposed code is improved.

2 Recursive constructions

We shall use the following standard recursive constructions. The proofs of these constructions can be found in [7].

Construction 2.1 *(Weighting) Let* $(X, \mathcal{G}, \mathcal{B})$ *be a super-simple GDD with index* λ_1*, and let* $w : X \to Z^+ \cup \{0\}$ *be a weight function on* X*, where* Z^+ *is the set of positive integers. Suppose that for each block* $B \in \mathcal{B}$*, there exists a super-simple* (k, λ_2)*-GDD of type* $\{w(x) : x \in B\}$*. Then there exists a super-simple* $(k, \lambda_1\lambda_2)$*-GDD of type* $\{\sum_{x \in G_i} w(x) : G_i \in \mathcal{G}\}$.

Construction 2.2 *(Breaking up groups) If there exists a super-simple* (k, λ)*-GDD of type* $h_1^{u_1} \cdots h_t^{u_t}$ *and a super-simple* $(h_i + \eta, k, \lambda)$*-BIBD for each* i $(1 \le i \le t)$*, then there exists a super-simple* $(\sum_{i=1}^{t} h_i u_i + \eta, k, \lambda)$*-BIBD, where* $\eta = 0$ *or* 1*.*

A *transversal design*, TD$(k, \lambda; n)$, is a (k, λ)-GDD of group type n^k and block size k. When $\lambda = 1$, we simply write TD(k, n). It is well known that a TD(k, n) is equivalent to $k - 2$ mutually orthogonal Latin squares (MOLS) of order n. For a list of lower bounds on the number of MOLS for orders up to 10000, we refer the reader to [1]. We shall denote by $N(n)$ the maximum number of MOLS of order n. In this paper, we shall employ the following known results on TDs.

Lemma 2.3 ([1])

1. A TD$(q + 1, q)$ *exists, consequently, a TD*(k, q) *exists for any positive integer* k $(k \le q + 1)$*, where* q *is a prime power.*

2. A TD$(7, n)$ *exists for all* $n \ge 63$*.*

3 Direct constructions

We shall use direct constructions to obtain super-simple $(v, 5, 4)$-BIBDs for some small values of v and some super-simple $(5, 4)$-GDDs, which will be used as master designs or input designs in our recursive constructions. All of these designs have been found after computer searches. The checking for super-simplicity can be done by computer after developing the designs.

In computer searching, we used a method which we called a "shuffling and backtracking" algorithm. This program consists of two parts. One part is a standard backtracking algorithm used to find base blocks. The other part is a shuffling algorithm which shuffles the blocks already found. So this is not an exhaustive search. A start point is set for the shuffling algorithm. For example, if there are 15 base blocks should be found, then we may set the start point at 5. That means the shuffling algorithm will be called after 5 base blocks have been found. A simple shuffling algorithm just exchanges two blocks. However, we will set the frequency of the calling shuffling algorithm. In our experience, to choose the start point and the appropriate frequency is important for the success of the search.

In what follows we use the notation "$+d \pmod v$", which denotes that all elements of the base blocks should be developed cyclically by adding $d \pmod v$ to them, while the infinite point ∞, if it occurs in the base blocks, is always fixed. We usually omit $+d$ when $d = 1$.

Let $[a, b]_5^{0,1}$ be the set of positive integers v such that $v \equiv 0, 1 \pmod 5$ and $a \le v \le b$. $[a, b)_5^{0,1}$ is similarly defined. To prove Theorem 1.3 we need to prove that there exists a $(v, 5, 4)$-BIBD for all $v \in [15, \infty)_5^{0,1}$.

Lemma 3.1 *There exists a super-simple $(v, 5, 4)$-BIBD for any $v \in M = [15, 86]_5^{0,1} \cup \{95,$ 110, 111, 115, 116, 130, 131$\}$.*

Proof For each $v \in M$, we take point set $X = Z_{v-1} \cup \{\infty\}$ or $X = Z_v$ when $v \equiv 0$ or 1 (mod 5), respectively, and take block set $\mathcal{B}$ as follows. It is readily checked that $(X, \mathcal{B})$ is the required design.

$v = 15$: $\{0, 1, 2, 3, 8\}$, $\{0, 3, 9, 11, 13\}$, $\{0, 2, 4, 7, 11\}$, $\{0, 1, 4, 9, 10\}$, $\{0, 1, 5, 7, \infty\}$, $\{0, 2, 10, 13, \infty\}$ +2 mod 14.

$v = 16$: $\{0, 1, 3, 6, 8\}$, $\{1, 2, 7, 11, 14\}$, $\{0, 1, 2, 4, 5\}$, $\{0, 2, 7, 8, 12\}$, $\{0, 1, 7, 9, 10\}$, $\{0, 3, 5, 7, 11\}$ +2 mod 16.

$v = 20$: $\{0, 3, 4, 9, 16\}$, $\{0, 1, 9, 14, 18\}$, $\{0, 2, 4, 8, 11\}$, $\{0, 5, 7, 8, \infty\}$ mod 19.

$v = 21$: $\{0, 7, 10, 18, 19\}$, $\{0, 4, 9, 14, 15\}$, $\{0, 3, 6, 7, 8\}$, $\{0, 2, 4, 8, 16\}$ mod 21.

$v = 25$: $\{0, 5, 11, 21, 22\}$, $\{0, 1, 6, 9, 13\}$, $\{0, 1, 5, 7, 15\}$, $\{0, 1, 4, 10, 12\}$, $\{0, 2, 17, 21, \infty\}$ mod 24.

$v = 26$: $\{0, 5, 7, 13, 22\}$, $\{0, 11, 16, 19, 20\}$, $\{0, 3, 7, 19, 25\}$, $\{0, 8, 13, 14, 24\}$, $\{0, 1, 3, 12, 24\}$ mod 26.

$v = 30$: $\{0, 3, 16, 21, 23\}$, $\{0, 2, 10, 20, 25\}$, $\{0, 1, 2, 15, 26\}$, $\{0, 4, 9, 12, 26\}$, $\{0, 4, 10, 11, 27\}$, $\{0, 1, 8, 20, \infty\}$ mod 29.

$v = 31$: $3^i\{0, 1, 3, 7, 15\}$ mod 31, $0 \le i \le 5$.

$v = 35$: $\{0, 6, 7, 12, 30\}$, $\{0, 10, 18, 24, 31\}$, $\{0, 8, 23, 25, 32\}$, $\{0, 4, 5, 6, 21\}$, $\{0, 5, 8, 12, 20\}$, $\{0, 11, 20, 29, 32\}$, $\{0, 1, 4, 15, \infty\}$ mod 34.

$v = 36$: $\{0, 2, 3, 13, 27\}$, $\{0, 10, 11, 14, 30\}$, $\{0, 3, 10, 17, 34\}$, $\{0, 13, 18, 22, 26\}$, $\{0, 2, 9, 17, 30\}$, $\{0, 4, 5, 16, 34\}$, $\{0, 1, 6, 9, 21\}$ mod 36.

$v = 40$: $\{0, 5, 7, 8, 18\}$, $\{0, 11, 13, 27, 36\}$, $\{0, 2, 14, 17, 22\}$, $\{0, 6, 20, 24, 30\}$, $\{0, 3, 7, 26, 35\}$, $\{0, 12, 22, 30, 38\}$, $\{0, 1, 6, 18, 38\}$, $\{0, 4, 28, 33, \infty\}$ mod 39.

$v = 41$: $7^i\{0, 1, 4, 11, 29\}$ mod 41, $0 \le i \le 7$.

For the remaining values of v, their associated super-simple designs are presented in the Appendix. $\square$

The following super-simple GDDs will be used as master designs or input designs in our recursive constructions.

Lemma 3.2 *There exists a super-simple* $(5,4)$*-GDD of type* 5^5*.*

Proof Let $X = Z_{25}$ and let $\mathcal{G} = \{\{i, 5+i, 10+i, 15+i, 20+i\} : \ 0 \leq i \leq 4\}$. Take block set $\mathcal{B}$ as follows. It is readily checked that $(X, \mathcal{B}, \mathcal{G})$ is the required design.

$\{0,4,21,22,23\}$, $\{3,9,12,15,21\}$, $\{2,6,10,18,19\}$, $\{0,1,18,22,24\}$, $\{0,7,13,14,21\}$,
$\{0,2,9,11,23\}$, $\{3,6,9,17,20\}$, $\{0,2,6,8,24\}$, $\{0,12,16,23,24\}$, $\{0,1,9,12,13\}$,
$\{1,2,10,14,23\}$, $\{0,6,7,9,18\}$, $\{3,10,14,21,22\}$, $\{4,5,8,16,22\}$, $\{4,6,10,12,13\}$,
$\{0,1,3,4,7\}$, $\{0,3,6,12,14\}$, $\{0,7,8,16,19\}$, $\{3,5,6,22,24\}$, $\{0,2,14,16,18\}$ $+5 \bmod 25$. □

Lemma 3.3 *For each* t*,* $6 \leq t \leq 10$*, there exists a super-simple* $(5,4)$*-GDD of type* 5^t*.*

Proof Let the point set be Z_{5t} and let the group set be $\{\{i, t+i, 2t+i, 3t+i, 4t+i\} : \ 0 \leq i \leq t-1\}$. Bellow are the required base blocks:

$t = 6$:
$\{0,2,7,10,17\}$, $\{0,19,20,21,28\}$, $\{0,11,21,25,26\}$, $\{0,9,13,16,17\}$, $\{0,2,16,19,27\}$.

$t = 7$:
$\{0,1,30,31,33\}$, $\{0,11,15,20,23\}$, $\{0,10,19,25,27\}$, $\{0,4,16,22,33\}$, $\{0,9,18,19,22\}$,
$\{0,1,12,20,25\}$.

$t = 8$:
$\{0,2,6,13,28\}$, $\{0,3,10,17,31\}$, $\{0,6,11,20,33\}$, $\{0,5,22,25,28\}$, $\{0,1,5,10,11\}$,
$\{0,1,2,4,23\}$, $\{0,2,12,27,31\}$.

$t = 9$:
$\{0,16,17,30,32\}$, $\{0,3,4,20,41\}$, $\{0,11,26,32,37\}$, $\{0,6,31,39,44\}$, $\{0,2,30,33,37\}$,
$\{0,14,17,19,24\}$, $\{0,10,11,21,33\}$, $\{0,2,22,25,41\}$.

$t = 10$:
$\{0,12,21,25,33\}$, $\{0,2,18,23,45\}$, $\{0,3,11,12,26\}$, $\{0,13,17,28,36\}$, $\{0,11,16,17,35\}$,
$\{0,6,7,32,43\}$, $\{0,2,5,38,46\}$, $\{0,3,31,47,49\}$, $\{0,2,21,28,37\}$.

Here, All the above base blocks are developed by $\bmod 5t$. □

Lemma 3.4 *There exists a super-simple* $(5,4)$*-GDD of type* $(15)^t$ *for* $t \in T = \{6,7,9\}$*.*

Proof For each $t \in T$, we construct a super-simple $(5,4)$-GDD of type $(15)^t$. Let the point set be Z_{15t} and let the group set be $\{\{i, t+i, 2t+i, \cdots, 14t+i\} : 0 \leq i \leq t-1\}$. The base blocks are listed below. Here, all the base blocks are developed by $\bmod 15t$.

$t=6$: $7^i\{0,1,15,32,83\}$, $7^i\{0,16,25,69,74\}$, $7^i\{0,10,33,43,71\}$, $0 \le i \le 2$, $\{0,15,16,43,56\}$, $\{0,10,55,69,80\}$, $\{0,23,55,63,76\}$, $\{0,1,57,77,82\}$, $\{0,2,81,85,88\}$.

$t=7$: $\{0,31,57,75,76\}$, $\{0,50,55,72,102\}$, $\{0,27,40,93,99\}$, $\{0,66,74,82,93\}$, $\{0,10,11,85,100\}$, $\{0,22,26,59,60\}$, $\{0,62,64,81,101\}$, $\{0,34,73,81,99\}$, $\{0,1,19,44,76\}$, $\{0,5,53,69,94\}$, $\{0,22,58,68,76\}$, $\{0,31,37,82,102\}$, $\{0,69,92,96,101\}$, $\{0,51,54,92,94\}$, $\{0,15,73,82,95\}$, $\{0,43,45,81,93\}$, $\{0,44,46,61,71\}$, $\{0,3,55,79,88\}$.

$t=9$: $2^i\{0,1,2,5,24\}$, $2^i\{0,3,13,20,46\}$, $2^i\{0,7,22,51,110\}$, $2^i\{0,7,46,85,116\}$, $0 \le i \le 3$, $\{0,11,32,66,134\}$, $\{0,23,65,76,105\}$, $\{0,33,52,91,120\}$, $\{0,23,74,87,98\}$, $\{0,23,58,71,84\}$, $\{0,46,61,123,125\}$, $\{0,25,55,60,85\}$, $\{0,6,22,38,107\}$. ▯

4 Proof of Theorem 1.3

In this section, we give the proof of our main theorem using direct constructed designs and recursive methods discussed in previous sections.

Lemma 4.1 *There exists a super-simple* $(v,5,4)$*-BIBD for any* $v \in M = \{100,\ 101,\ 120,\ 121,\ 140,\ 141,\ 160,\ 161,\ 180,\ 181\}$.

Proof For each $v \in M$, we can write $v = 20t + \eta$, where $t \in \{5,6,7,8,9\}$, $\eta = 0$ or 1. Starting from a super-simple $(5,4)$-GDD of type 5^t coming from Lemma 3.2 and Lemma 3.3, and applying Construction 2.1 with a TD$(5,4)$ coming from Lemma 2.3, we obtain a super-simple $(5,4)$-GDD of type $(20)^t$. Since there exists a super-simple $(20+\eta,5,4)$-BIBD, by Construction 2.2 we obtain a super-simple $(20t+\eta,5,4)$-BIBD. ▯

Lemma 4.2 *There exists a super-simple* $(v,5,4)$*-BIBD for any* $v \in M = \{125,\ 126,\ 145,\ 146,\ 150,\ 151\}$.

Proof For each $v \in M$, we can write $v = 125 + 5a + \eta$, where $a \in \{0,4,5\}$, $\eta = 0$ or 1. By removing $5-a$ points from the last group of a TD$(6,5)$ coming from Lemma 2.3 we obtain a $\{5,6\}$-GDD of type 5^5a^1. Applying Construction 2.1 with weight 5, we obtain a super-simple $(5,4)$-GDD of type $(25)^5(5a)^1$. Here, the input super-simple $(5,4)$-GDDs of types 5^5 and 5^6 come from Lemma 3.2 and Lemma 3.3, respectively. Since there exists a super-simple $(25+\eta,5,4)$-BIBD and a super-simple $(5a+\eta,5,4)$-BIBD, by Construction 2.2 we get a super-simple $(125+5a+\eta,5,4)$-BIBD. ▯

Lemma 4.3 *There exists a super-simple* $(v, 5, 4)$*-BIBD for any* $v \in \{155,\ 156\}$.

Proof By Theorem 1.2 in [9], there exists a 4-RGDD of group type 3^8, which has seven parallel classes. Add seven "new" points to the above RGDD we obtain a 5-GDD of type $3^8 7^1$. Starting from this GDD and applying Construction 2.1 with weight 5, we obtain a super-simple $(5, 4)$-GDD of type $(15)^8(35)^1$. Here, the input super-simple $(5, 4)$-GDD of type 5^5 comes from Lemma 3.2. Since there exists a super-simple $(15+\eta, 5, 4)$-BIBD and a super-simple $(35 + \eta, 5, 4)$-BIBD, by Construction 2.2 we get a super-simple $(155 + \eta, 5, 4)$-BIBD, where $\eta = 0$ or 1. $\square$

Lemma 4.4 *There exists a super-simple* $(v, 5, 4)$*-BIBD for any* $v \in \{170,\ 171,\ 175,\ 176,\ 185,\ 186\}$.

Proof For $v \in \{170, 171\}$, starting from a TD$(8, 7)$ coming from Lemma 2.3, select three blocks intersecting at the last group and delete all points of these three blocks, we obtain a $\{5, 6, 7, 8\}$-GDD of type $4^7 6^1$. Applying Construction 2.1 with weight 5, we obtain a super-simple $(5, 4)$-GDD of type $(20)^7(30)^1$. Here, the input super-simple $(5, 4)$-GDD of type $5^5, 5^6, 5^7$ and 5^8 come from Lemma 3.2 and Lemma 3.3. Since there exists a super-simple $(20 + \eta, 5, 4)$-BIBD and a super-simple $(30 + \eta, 5, 4)$-BIBD, by Construction 2.2 we get a super-simple $(170 + \eta, 5, 4)$-BIBD, where $\eta = 0$ or 1.

For $v \in \{175, 176\}$, starting from a TD$(8, 7)$ coming from Lemma 2.3 and applying Construction 2.1 with a super-simple $(5, 4)$-GDD of type 5^8 coming from Lemma 3.3, we obtain a super-simple $(5, 4)$-GDD of type $(35)^5$. Since there exists a super-simple $(35+\eta, 5, 4)$-BIBD, by Construction 2.2 we get a super-simple $(175 + \eta, 5, 4)$-BIBD, where $\eta = 0$ or 1.

For $v \in \{185, 186\}$, starting from a TD$(7, 7)$ coming from Lemma 2.3, select two blocks intersecting at the last group and delete all other points of these two blocks except for the common one, we obtain a $\{5, 6, 7\}$-GDD of type $5^6 7^1$. Applying Construction 2.1 with weight 5, we obtain a super-simple $(5, 4)$-GDD of type $25^6 35^1$. Here, the input super-simple $(5, 4)$-GDD of type $5^5, 5^6$ and 5^7 come from Lemma 3.2 and Lemma 3.3. Since there exists a super-simple $(25 + \eta, 5, 4)$-BIBD and a super-simple $(35 + \eta, 5, 4)$-BIBD, by Construction 2.2 we get a super-simple $(185 + \eta, 5, 4)$-BIBD, where $\eta = 0$ or 1. $\square$

Lemma 4.5 *There exists a super-simple* $(v, 5, 4)$*-BIBD for any* $v \in M = \{90,\ 91,\ 105,\ 106,\ 135,\ 136\}$.

Proof For each $v \in M$, we can write $v = 15t+\eta$, where $t \in \{6,7,9\}$, $\eta = 0$ or 1. Since there exist a super-simple $(5,4)$-GDD of type $(15)^t$ coming from Lemma 3.4 and a super-simple $(15+\eta,5,4)$-BIBD, by Construction 2.2 we obtain a super-simple $(15t+\eta,5,4)$-BIBD. ▯

Lemma 4.6 *There exists a super-simple* $(96,5,4)$*-BIBD.*

Proof A super-simple $(5,4)$-GDD of group type 4^6 is shown as follows. $X = Z_{24}$, $\mathcal{G} = \{\{i, 6+i, 12+i, 18+i\} : 0 \leq i \leq 5\}$, $\mathcal{B} = \{\{0,1,2,4,11\}, \{0,1,5,15,22\}, \{0,1,9,16,20\}, \{0,2,13,16,21\} \bmod 24\}$.

Starting from this GDD and applying Construction 2.1 with a TD$(5,4)$ coming from Lemma 2.3, we obtain a super-simple $(5,4)$-GDD of type $(16)^6$. Since there exists a super-simple $(16,5,4)$-BIBD, by Construction 2.2 we get a super-simple $(96,5,4)$-BIBD. ▯

Lemma 4.7 *There exists a super-simple* $(v,5,4)$*-BIBD for any* $v \in \{165,\ 166\}$.

Proof Let $X = Z_{33}$, $\mathcal{G} = \{\{i, 11+i, 22+i\} :\ 0 \leq i \leq 10\}$ and $\mathcal{B} = \{\{0,2,3,6,27\}, \{0,9,15,19,29\}, \{0,2,10,19,26\}, \{0,1,8,13,20\}, \{0,4,5,6,21\}, \{0,2,5,15,30\} \bmod 33\}$. It is readily checked that $(X,\mathcal{G},\mathcal{B})$ is a super-simple $(5,4)$-GDD of type 3^{11}. Starting from this GDD and applying Construction 2.1 with a TD$(5,5)$ coming from Lemma 2.3 to obtain a super-simple $(5,4)$-GDD of type $(15)^{11}$. Since there exists a super-simple $(15+\eta,5,4)$-BIBD, by Construction 2.2 we get a super-simple $(165+\eta,5,4)$-BIBD, where $\eta = 0$ or 1. ▯

So far, we have proved that there exists a super-simple $(v,5,4)$-BIBD for every $v \in [15,186]_5^{0,1}$. Next, we shall show that there exists a super-simple $(v,5,4)$-BIBD for any $v \in [190,1591]_5^{0,1}$.

Lemma 4.8 *Suppose* $k \in \{5,6,7,8,9,10\}$*. Let* $N(m) \geq k-2$*,* $r = k-5$ *and let* $M = \{5m,\ 5a_1,\ \cdots,\ 5a_r\}$*, where* $a_i \in [3,m] \cup \{0\}$*,* $1 \leq i \leq r$*. If there exists a super-simple* $(u+\eta,5,4)$*-BIBD for any* $u \in M$*, then there exists a super-simple* $(v,5,4)$*-BIBD, where* $v = 25m + 5\sum_{i=1}^{r} a_i + \eta$*,* $\eta = 0$ *or* 1.

Proof By removing $m - a_i$ $(i = 1,\cdots,r)$ points from the last r groups of a TD(k,m) respectively, we get a $\{5,6,\cdots,k\}$-GDD of type $m^5 a_1^1 a_2^1 \cdots a_r^1$. Starting from this GDD and applying Construction 2.1 with weight 5, we obtain a super-simple $(5,4)$-GDD of type $(5m)^5(5a_1)^1\cdots(5a_r)^1$. Here, the input super-simple $(5,4)$-GDDs of types 5^t with $t\in\{5,6,\cdots,k\}$ come from Lemma 3.2 and Lemma 3.3. Since there exists a super-simple $(u+\eta,5,4)$-BIBD for any $u\in M$, by Construction 2.2 we get a super-simple $(25m+5\sum_{i=1}^{r}a_i+\eta,5,4)$-BIBD. ∎

Lemma 4.9 *There exists a super-simple* $(v,5,4)$*-BIBD for any* $v\in[190,1591]_5^{0,1}$.

Proof Applying Lemma 4.8 with parameters in the following table, we obtain a super-simple $(v,5,4)$-BIBD for every $v\in[190,1591]_5^{0,1}$. All TD(k,m) used here come from Lemma 2.3.

$v=25m+5\sum_{i=1}^{k-5}a_i+\eta$	m	k	$\sum_{i=1}^{k-5}a_i$	η
$[190,281]_5^{0,1}$	7	8	$[3,21]$	$\{0,1\}$
$[285,451]_5^{0,1}$	9	10	$[12,45]$	$\{0,1\}$
$[455,651]_5^{0,1}$	13	10	$[26,65]$	$\{0,1\}$
$[655,1251]_5^{0,1}$	25	10	$[6,125]$	$\{0,1\}$
$[1255,1591]_5^{0,1}$	36	10	$[71,138]$	$\{0,1\}$

Theorem 4.10 *There exists a super-simple* $(v,5,4)$*-BIBD for all* $v\in[15,\infty)_5^{0,1}$.

Proof The proof is by induction on v. In view of the above lemmas, we can assume $v\geq 1595$. We can write $v=25m+5(a_1+a_2)+\eta$, where $m\geq 63$, $\eta=0,1$, $\{a_1,a_2\}\subset[3,m]\cup\{0\}$ and $a_1+a_2\in[3,2m]$. Since $N(m)\geq 5$, by induction there exists a super-simple $(5m+\eta,5,4)$-BIBD and a super-simple $(5a_i+\eta,5,4)$-BIBD, $i=1,2$, we know that there exists a super-simple $(v,5,4)$-BIBD by Lemma 4.8. ∎

By the above discussion, we have complete the proof of Theorem 1.3.

5 Conclusion and Remark

It is proved in this paper that the necessary condition for the existence of a super-simple $(v,5,4)$-BIBD is also sufficient. In the proof, some designs are given by direct constructions. Those designs are obtained by a shuffling and backtracking algorithm. Actually, we also used this algoritm to find some super-simple $(v, 5, 2)$-BIBDs. More precisely, we constructed super-simple $(v, 5, 2)$-BIBDs for $v = 75, 95, 385$, which are three of the eleven unsettled cases listed in Theorem 1.2.

Lemma 5.1 *There exists a super-simple* $(v, 5, 2)$*-BIBD for every* $v \in \{75, 95\}$.

Proof: For each $v \in \{75, 95\}$, let the point set be $Z_{v-1} \cup \{\infty\}$. Bellow are the required base blocks.

$v = 75$:
$\{0, 4, 25, 37, 60\}$, $\{0, 29, 52, 63, 64\}$, $\{0, 50, 58, 59, 69\}$, $\{0, 7, 60, 61, 65\}$, $\{0, 17, 31, 42, 48\}$, $\{1, 3, 25, 27, 43\}$, $\{1, 5, 26, 43, 69\}$, $\{1, 13, 19, 52, 56\}$, $\{1, 2, 9, 29, 37\}$, $\{0, 13, 20, 32, 40\}$, $\{0, 2, 27, 30, 48\}$, $\{0, 22, 45, 58, 67\}$, $\{1, 6, 46, 61, 70\}$, $\{0, 3, 6, 44, 47\}$, $\{0, 2, 15, 59, \infty\}$.

$v = 95$:
$\{1, 48, 55, 57, 81\}$, $\{1, 9, 18, 29, 58\}$, $\{0, 6, 66, 67, 83\}$, $\{1, 13, 53, 77, 80\}$, $\{0, 19, 40, 52, 90\}$, $\{0, 2, 41, 48, 66\}$, $\{0, 49, 53, 68, 84\}$, $\{0, 20, 23, 24, 55\}$, $\{1, 9, 10, 62, 81\}$, $\{1, 44, 52, 66, 88\}$, $\{1, 35, 58, 74, 85\}$, $\{1, 13, 49, 60, 78\}$, $\{0, 2, 5, 10, 89\}$, $\{0, 6, 36, 49, 62\}$, $\{0, 5, 21, 24, 81\}$, $\{0, 25, 31, 62, 74\}$, $\{1, 37, 43, 63, 65\}$, $\{0, 9, 13, 34, 59\}$, $\{0, 1, 39, 80, \infty\}$.

Here, all the above base blocks are developed by $+2 \bmod v - 1$. $\square$

Lemma 5.2 *There exists a super-simple* $(385, 5, 2)$*-BIBD.*

Proof: Let $X = Z_{35}$ and let $\mathcal{G} = \{\{i, 7+i, 14+i, 21+i, 28+i\} : 0 \leq i \leq 6\}$ and $\mathcal{B} = \{\{0, 9, 10, 27, 33\}, \{0, 3, 11, 15, 16\} \{0, 2, 5, 15, 31\} \bmod 35\}$. It is readily checked that $(X, \mathcal{G}, \mathcal{B})$ is a super-simple $(5, 2)$-GDD of type 5^7.

Starting from a TD$(7, 11)$ coming from Lemma 2.3 and applying Construction 2.1 with a super-simple $(5, 2)$-GDD of type 5^7 to obtain a super-simple $(5, 2)$-GDD of type $(55)^7$. Since there exists a super-simple $(55, 5, 2)$-BIBD, by Construction 2.2 we get a super-simple $(385, 5, 2)$-BIBD. $\square$

So we improved the result of Theorem 1.2 and now rewrite it in the following.

Theorem 5.3 *A super-simple* $(v, 5, 2)$*-BIBD exists if and only if* $v \equiv 1, 5 \pmod{10}$, $v \neq 5, 15$, *except possibly when* $v \in \{115, 135, 195, 215, 231, 285, 365, 515\}$.

As stated in Kim and Lebedev [13], super-simple designs can be used to construct superimposed codes. An $N \times T$ $(0,1)$-matrix C is called a (w,r) superimposed codes of size $N \times T$, if for any pair of subsets I, $J \subset [T] = \{1, 2, \cdots, T\}$ such that $|I| = w$, $|J| = r$ and $I \cap J = \emptyset$ there exists a coordinate $x \in [N] = \{1, 2, \cdots, N\}$ such that $c_{xp} = 1$ for all $p \in I$ and $c_{xq} = 0$ for all $q \in J$.

The main problem in the study of superimposed codes is to find the minimal length $N(T; w, r)$ of a (w,r) superimposed code for a given cardinality T. The following result can be found in [13].

Lemma 5.4 *A super-simple (v,k,λ)-BIBD is a $(2, \lambda-1)$ superimposed code of $N \times v$, where $N = \frac{\lambda v(v-1)}{k(k-1)}$.*

Combining Lemma 5.4 with Theorem 1.3, we have the following.

Lemma 5.5 *For any $v \equiv 0, 1 \pmod 5$, $v \geq 15$, there exists $(2,3)$ superimposed code of $N \times v$, where $N = \frac{v(v-1)}{5}$.*

Remark: By Lemma 5.5, we have $N(v; 2, 3) \leq \frac{v(v-1)}{5}$. In particular, when $v = 15$, we have $N(15; 2, 3) \leq 42$, which improves the result $N(12; 2, 3) \leq 45$ presented in [13].

References

[1] R. J. R. Abel, A. E. Brouwer, C. J. Colbourn and J. H. Dinitz, Mutually orthogonal Latin squares, in: C.R.C. Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz, eds.), CRC Press, Boca Raton, FL., 1996, 111-142.

[2] P. Adams, D. Bryant and A. Khodkar, On the existence of super-simple designs with block size 4, Aequationes Math. 52 (1996), 230-246.

[3] I. Bluskov, New Designs, J. Combin. Math. Combin. Comput. 23 (1997), 212-220.

[4] I. Bluskov and H. Hämäläinen, New upper bounds on the minimum size of covering designs, J. Combin. Designs 6 (1998), 21-41.

[5] I. Bluskov and K. Heinrich, Super-simple designs with $v \leq 32$, J. Statist. Plann. Inference 95 (2001), 121-131.

[6] K. Chen, On the existence of super-simple $(v, 4, 3)$-BIBDs, J. Combin. Math. Combin. Comput. 17 (1995), 149-159.

[7] K. Chen, On the existence of super-simple $(v, 4, 4)$-BIBDs, J. Statist. Plann. Inference 51 (1996), 339-350.

[8] K. Chen, Z. Cao and R. Wei, Super-simple balanced incomplete block designs with block size 4 and index 6, J. Statist. Plann. Inference, to appear.

[9] G. Ge and A.C.H. Ling, A survey on resolvable group divisible designs with block size four, Discrete Math. 279 (2004), 225-245.

[10] H.-D. O. F. Gronau and R. C. Mullin, On super-simple $2-(v, 4, \lambda)$ designs, J. Combin. Math. Combin. Comput. 11 (1992), 113-121.

[11] H.-D. O. F. Gronau, D. L. Kreher and A. C. H. Ling, Super-simple $(v, 5, 2)$-designs, Discrete Applied Mathematics 138 (2004), 65-77.

[12] A. Khodkar, Various super-simple designs with block size four, Australas. J. Combin. 9 (1994), 201-210.

[13] H. K. Kim and V. Lebedev, On optimal superimposed codes, J. Combin. Designs 12 (2004), 79-91.

[14] D. R. Stinson, R. Wei and L. Zhu, New Constructions for perfect hash families and related structures using related combinatorial designs and codes, J. Combin. Designs 8 (2000), 189-200.

Appendix

The values of v and blocks of super-simple $(v, 5, 4)$-BIBDs used in Lemma 3.1 are listed below.

v blocks

45: $\{0,4,10,12,23\}$, $\{0,1,3,19,29\}$, $\{0,5,24,36,41\}$, $\{0,18,32,38,39\}$, $\{0,14,16,36,43\}$, $\{0,2,7,11,21\}$, $\{0,9,26,40,43\}$, $\{0,9,22,33,37\}$, $\{0,3,9,32,\infty\}$ mod 44.

46: $\{0,1,7,10,14\}$, $\{0,12,24,26,32\}$, $\{0,25,28,29,31\}$, $\{0,5,22,24,45\}$, $\{0,10,15,28,37\}$, $\{0,23,30,34,42\}$, $\{0,2,7,16,33\}$, $\{0,17,25,35,38\}$, $\{0,1,20,31,36\}$ mod 46.

50: $2^i\{0,8,15,47,48\}$, $2^i\{0,5,19,42,45\}$, $0 \le i \le 2$, $\{0,1,3,23,31\}$, $\{0,5,12,25,36\}$, $\{0,5,17,27,43\}$, $\{0,5,14,39,\infty\}$ mod 49.

51: $\{0,17,22,29,40\}$, $\{0,17,27,30,32\}$, $\{0,20,33,39,50\}$, $\{0,5,27,35,42\}$, $\{0,2,16,28,42\}$, $\{0,24,30,47,50\}$, $\{0,15,18,31,47\}$, $\{0,6,32,42,44\}$, $\{0,5,7,8,50\}$, $\{0,4,8,31,41\}$ mod 51.

55: $\{0,3,15,25,53\}$, $\{0,6,8,28,31\}$, $\{0,6,17,33,52\}$, $\{0,7,14,22,40\}$, $\{0,6,21,42,44\}$, $\{0,4,13,18,30\}$, $\{0,5,9,13,16\}$, $\{0,20,30,31,45\}$, $\{0,5,22,34,35\}$, $\{0,2,3,20,47\}$, $\{0,5,11,24,\infty\}$ mod 54.

56: $\{0,9,11,25,34\}$, $\{0,21,39,40,41\}$, $\{0,15,20,23,28\}$, $\{0,6,7,29,46\}$, $\{0,10,42,45,53\}$, $\{0,2,4,32,36\}$, $\{0,11,26,44,51\}$, $\{0,12,41,46,47\}$, $\{0,6,13,20,32\}$, $\{0,9,13,27,30\}$, $\{0,4,10,29,48\}$ mod 56.

60: $2^i\{0,1,4,10,52\}$, $0 \le i \le 7$, $\{0,1,3,17,34\}$, $\{0,2,5,37,41\}$, $\{0,6,19,31,52\}$, $\{0,14,23,44,\infty\}$ mod 59.

61: $2^i\{0,1,3,21,55\}$ mod 61, $0 \le i \le 11$.

65: $\{0,10,23,25,39\}$, $\{0,20,22,23,48\}$, $\{0,19,23,51,53\}$, $\{0,19,25,46,49\}$, $\{0,5,27,35,36\}$, $\{0,7,16,45,56\}$, $\{0,31,37,51,57\}$, $\{0,4,44,49,56\}$, $\{0,5,7,47,53\}$, $\{0,1,10,22,27\}$, $\{0,14,28,32,61\}$, $\{0,9,10,13,56\}$, $\{0,31,41,52,\infty\}$ mod 64.

66: $\{0,17,36,37,65\}$, $\{0,5,15,24,27\}$, $\{0,16,32,33,54\}$, $\{0,4,20,22,27\}$, $\{0,39,45,47,58\}$, $\{0,6,32,34,59\}$, $\{0,10,17,25,43\}$, $\{0,6,29,42,63\}$, $\{0,5,9,35,57\}$, $\{0,20,24,31,62\}$, $\{0,29,35,43,45\}$, $\{0,3,14,15,55\}$, $\{0,3,13,49,54\}$ mod 66.

70: $\{0,26,33,52,64\}$, $\{0,5,25,43,59\}$, $\{0,18,37,47,65\}$, $\{0,9,29,33,50\}$, $\{0,30,35,36,37\}$, $\{0,9,11,51,59\}$, $\{0,22,49,52,55\}$, $\{0,4,6,12,58\}$, $\{0,9,23,38,62\}$, $\{0,13,16,21,43\}$, $\{0,23,32,44,57\}$, $\{0,4,20,27,28\}$, $\{0,1,15,56,59\}$, $\{0,2,13,37,\infty\}$ mod 69.

71: $13^i\{0,1,6,14,31\}$ mod 71, $0 \le i \le 13$.

75: $\{0,19,25,30,47\}$, $\{0,1,5,57,73\}$, $\{0,18,20,36,47\}$, $\{0,8,40,55,60\}$, $\{0,4,33,37,55\}$, $\{0,10,30,39,65\}$, $\{0,12,25,28,65\}$, $\{0,24,31,65,72\}$, $\{0,21,36,60,61\}$, $\{0,1,32,46,49\}$, $\{0,3,14,38,64\}$, $\{0,16,23,28,31\}$, $\{0,36,44,51,57\}$, $\{0,21,32,44,64\}$, $\{0,4,66,68,\infty\}$ mod 74.

76: $\{0,30,42,68,74\}$, $\{0,17,36,58,71\}$, $\{0,5,7,58,65\}$, $\{0,5,51,55,67\}$, $\{0,15,27,42,56\}$, $\{0,1,9,22,67\}$, $\{0,5,6,12,45\}$, $\{0,37,38,48,63\}$, $\{0,3,4,23,52\}$, $\{0,20,36,53,55\}$, $\{0,29,37,52,73\}$, $\{0,6,10,52,54\}$, $\{0,17,26,30,33\}$, $\{0,11,45,56,73\}$, $\{0,8,27,37,51\}$ mod 76.

80: $\{0,23,29,33,65\}$, $\{0,41,53,66,71\}$, $\{0,4,40,49,64\}$, $\{0,20,22,54,73\}$, $\{0,20,37,68,70\}$, $\{0,4,7,16,52\}$, $\{0,20,21,28,38\}$, $\{0,8,11,32,33\}$, $\{0,12,21,35,62\}$, $\{0,40,44,50,51\}$, $\{0,2,17,44,76\}$, $\{0,45,48,56,61\}$, $\{0,39,40,61,63\}$, $\{0,37,53,67,72\}$, $\{0,13,19,43,65\}$, $\{0,10,38,64,\infty\}$ mod 79.

81: $\{0,26,30,47,49\}$, $\{0,27,38,65,79\}$, $\{0,7,31,66,68\}$, $\{0,16,21,52,58\}$, $\{0,15,31,41,49\}$, $\{0,7,50,75,78\}$, $\{0,17,52,60,78\}$, $\{0,9,18,45,57\}$, $\{0,14,20,68,69\}$, $\{0,7,8,18,64\}$, $\{0,28,48,51,70\}$, $\{0,33,45,67,73\}$, $\{0,37,42,46,74\}$, $\{0,57,59,76,80\}$, $\{0,40,56,69,70\}$, $\{0,4,9,19,34\}$ mod 81.

85: $\{0,4,7,60,82\}$, $\{0,11,25,48,68\}$, $\{0,25,41,57,58\}$, $\{0,10,15,45,75\}$, $\{0,18,30,47,68\}$, $\{0,38,42,53,56\}$, $\{0,18,52,55,57\}$, $\{0,15,41,67,74\}$, $\{0,1,22,65,72\}$, $\{0,6,29,39,71\}$, $\{0,4,28,48,78\}$, $\{0,29,38,40,60\}$, $\{0,3,26,40,48\}$, $\{0,17,35,48,73\}$, $\{0,4,75,76,83\}$, $\{0,49,51,57,72\}$, $\{0,5,19,40,\infty\}$ mod 84.

86: $\{0,41,68,69,72\}$, $\{0,31,33,59,84\}$, $\{0,7,43,63,78\}$, $\{0,21,22,77,79\}$, $\{0,24,30,44,78\}$, $\{0,5,18,39,43\}$, $\{0,23,41,47,50\}$, $\{0,26,36,65,78\}$, $\{0,10,70,72,82\}$, $\{0,5,27,37,46\}$, $\{0,17,28,46,70\}$, $\{0,12,13,64,67\}$, $\{0,16,19,42,65\}$, $\{0,38,49,74,79\}$, $\{0,8,69,75,82\}$, $\{0,20,66,71,77\}$, $\{0,1,17,39,54\}$ mod 86.

95: $\{0,19,25,58,63\}$, $\{0,21,38,73,81\}$, $\{0,12,22,43,80\}$, $\{0,64,69,80,82\}$, $\{0,16,31,40,88\}$, $\{0,3,23,43,50\}$, $\{0,48,59,67,92\}$, $\{0,1,3,36,77\}$, $\{0,3,52,68,86\}$, $\{0,49,53,77,84\}$, $\{0,1,4,13,40\}$, $\{0,1,8,38,72\}$, $\{0,21,30,53,70\}$, $\{0,23,28,32,70\}$, $\{0,26,37,55,88\}$, $\{0,10,14,79,89\}$, $\{0,7,46,48,75\}$, $\{0,12,13,28,62\}$, $\{0,6,20,72,\infty\}$ mod 94.

110: $\{0,30,34,43,101\}$, $\{0,19,36,83,103\}$, $\{0,46,57,74,98\}$, $\{0,73,78,85,100\}$, $\{0,1,44,50,67\}$, $\{0,21,59,86,89\}$, $\{0,23,48,63,104\}$, $\{0,33,46,53,87\}$, $\{0,61,71,74,108\}$, $\{0,26,51,80,96\}$, $\{0,4,14,70,81\}$, $\{0,1,32,37,63\}$, $\{0,15,75,94,108\}$, $\{0,40,85,88,97\}$, $\{0,8,55,65,84\}$, $\{0,6,27,33,97\}$, $\{0,59,77,79,81\}$, $\{0,31,38,40,48\}$, $\{0,32,36,50,85\}$, $\{0,18,26,40,98\}$, $\{0,37,86,102,107\}$, $\{0,3,19,54,\infty\}$ mod 109.

111: $\{0,8,80,85,104\}$, $\{0,33,68,69,76\}$, $\{0,55,57,87,97\}$, $\{0,23,39,52,96\}$, $\{0,3,20,86,107\}$, $\{0,6,27,77,79\}$, $\{0,33,34,86,108\}$, $\{0,51,63,64,91\}$, $\{0,5,68,79,105\}$, $\{0,38,61,65,83\}$, $\{0,36,53,56,80\}$, $\{0,11,33,79,93\}$, $\{0,5,41,51,107\}$, $\{0,28,44,104,110\}$, $\{0,47,57,88,103\}$, $\{0,47,49,58,72\}$, $\{0,20,33,82,90\}$, $\{0,69,81,95,99\}$, $\{0,12,17,38,47\}$, $\{0,50,53,63,69\}$, $\{0,15,40,59,77\}$, $\{0,2,19,41,50\}$ mod 111.

115: $\{0,34,79,93,100\}$, $\{0,15,42,62,108\}$, $\{0,23,56,75,84\}$, $\{0,24,29,51,100\}$, $\{0,36,44,76,86\}$, $\{0,1,11,106,109\}$, $\{0,18,50,87,106\}$, $\{0,9,37,75,92\}$, $\{0,53,102,111,113\}$, $\{0,12,79,82,102\}$, $\{0,1,16,46,74\}$, $\{0,30,42,43,50\}$, $\{0,7,11,74,85\}$, $\{0,30,34,51,101\}$, $\{0,4,6,29,83\}$, $\{0,2,35,89,92\}$, $\{0,5,18,54,71\}$, $\{0,10,41,65,109\}$, $\{0,19,34,52,72\}$, $\{0,68,75,97,101\}$, $\{0,57,80,98,112\}$, $\{0,10,26,51,88\}$, $\{0,6,31,75,\infty\}$ mod 114.

116: $\{0,1,67,88,94\}$, $\{0,54,63,68,101\}$, $\{0,55,62,99,100\}$, $\{0,8,11,42,65\}$, $\{0,11,16,35,67\}$, $\{0,24,89,99,103\}$, $\{0,23,25,37,61\}$, $\{0,47,77,85,90\}$, $\{0,5,12,16,99\}$, $\{0,4,34,74,102\}$, $\{0,26,41,107,114\}$, $\{0,28,39,72,97\}$, $\{0,18,64,71,74\}$, $\{0,20,36,40,99\}$, $\{0,19,55,73,86\}$, $\{0,9,12,34,98\}$, $\{0,20,35,41,60\}$, $\{0,41,56,87,113\}$, $\{0,1,33,46,69\}$, $\{0,12,51,71,106\}$, $\{0,39,63,106,115\}$, $\{0,66,68,74,95\}$, $\{0,50,82,108,114\}$ mod 116.

130: $\{0,18,45,82,110\}$, $\{0,11,21,34,82\}$, $\{0,8,52,93,108\}$, $\{0,54,57,59,108\}$, $\{0,26,50,53,94\}$, $\{0,11,83,114,123\}$, $\{0,3,69,70,112\}$, $\{0,57,79,122,124\}$, $\{0,21,40,95,120\}$, $\{0,12,49,63,110\}$, $\{0,39,69,75,92\}$, $\{0,11,23,85,127\}$, $\{0,5,30,38,114\}$, $\{0,36,40,52,56\}$, $\{0,24,32,46,122\}$, $\{0,41,74,101,124\}$, $\{0,36,79,95,101\}$, $\{0,16,26,67,97\}$, $\{0,15,42,105,122\}$, $\{0,7,10,20,101\}$, $\{0,18,19,91,100\}$, $\{0,1,32,33,116\}$, $\{0,12,71,75,127\}$, $\{0,35,39,68,77\}$, $\{0,11,71,105,111\}$, $\{0,8,26,51,\infty\}$ mod 129.

131: $2^i\{0,1,17,59,70\}$ mod 131, $0 \le i \le 25$.