Concerning the Generating Set of $\mathbb{Z}_{\geq n}$

Alan C.H. Ling and Charles J. Colbourn
Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario
CANADA N2L 3G1

To Ralph Stanton on his Seventieth ($\pm\varepsilon$) Birthday

Abstract

The generating set of $\mathbb{Z}_{\geq n}$ is determined completely for $n \leq 8$, with the exception of the (46,6,1) design. Some general results are presented for larger values of n.

1 Introduction

A *pairwise balanced design* (or *PBD*) is a pair (V,$\mathcal{B}$) where

1. V is a finite set of points,
2. $\mathcal{B}$ is a collection of subsets of V called blocks,
3. every pair of distinct points of V occur in exactly one blocks.

We use the notation $PBD(v, K)$ when $|V| = v$ and $|B| \in K$ for all $B \in \mathcal{B}$. We denote $B(K)$=$\{v$: there exists a PBD(v,K)$\}$. A set S of positive integers is *PBD-closed* if the existence of a PBD(v, S) implies that v belongs to S. Let K be a PBD-closed set. Let G be a set of positive integers such that $K = B(G)$. Then G is a *generating set* for K. Let K be a PBD-closed set. An element $x \in K$ is *essential* in K if and only if $x \notin B(K\backslash\{x\})$, that is, if and only if there does not exist a PBD($x, K\backslash\{x\}$). An element $x \in K$ is *inessential* if x is not essential.

We denote by $[a, b]$ the set of integers $\{x : a \leq x \leq b\}$, and by $\mathbb{Z}_{\geq n}$ the set of integers $\{v : v \geq n\}$. In this paper we examine generating sets for $\mathbb{Z}_{\geq n}$.

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

1. $\mathcal{G}$ is a partition of X into subsets called *groups*.
2. $\mathcal{A}$ 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 a unique block.

The *group type* of a GDD$(X, \mathcal{G}, \mathcal{A})$ is a multiset $\{|G| : G \in \mathcal{G}\}$. We usually use exponential notation to describe group types: a group type $1^{i_1}2^{i_2}\dots n^{i_n}$ denotes i_1 occurrences of 1, i_2 occurrences of 2 and so on. As with PBDs, we say that a GDD is a K-GDD if $|A| \in K$ for every $A \in \mathcal{A}$. A *transversal design* $TD(k,n)$, is a $\{k\}$-GDD of type n^k and 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 of all orders up to 10000, see [1].

A *balanced incomplete block design (BIBD)* with index λ is a $PBD_\lambda(v,K)$ with K=$\{k\}$. We use the notation $B_\lambda(v,k)$ where $|B|$=k for all $B \in \mathcal{B}$. Again, when λ=1, we simply denote it by $B(v,k)$. If the blocks of the design, $B(v,k)$, can be partitioned into classes $C_1, C_2, \dots, C_m$ such that every point in V appears in exactly one block in each C_i for $i = 1, 2, \dots, m$, the design is called *resolvable* and is denoted by $RB(v,k)$.

Often we denote $B(K) = \{v :$ there exists a PBD$(v,K)\}$. Also, $B(k) = \{v :$ there exists a $B(v,k)\}$ and $RB(k) = \{v :$ there exists a $RB(v,k)\}$.

A *finite projective plane of order n*, $n \geq 2$, is a collection of $n+1$ subsets (called *lines*) of a n^2+n+1-set V points, such that every two points of V occur together in exactly one of the lines.

Theorem 1.1 *[4] If q is a power of a prime number, then there exists a projective plane of order q, denoted $PG(2,q)$.*

An *oval* of a projective plane of order n is a set of $n+1$ points such that no three are collinear. A *hyperoval* of a projective plane of order n is a set of $n+2$ points such that no three are collinear.

Theorem 1.2 *[4] Let π be $PG(2,q)$ where q is odd. Then π contains an oval.*

Theorem 1.3 *[4] Let π be $PG(2,q)$ where $q = 2^n$ and n is a positive integer. Then π contains a hyperoval.*

The existence of ovals (and hyperovals) in $PG(2,q)$ is very useful in constructing pairwise balanced designs:

Theorem 1.4 *[4] Let q be a prime power. Then for $0 \leq t \leq q+1$,*

1. $q^2 - t \in B(\{q-2, q-1, q\})$
2. $q^2 + q + 1 - t \in B(\{q-1, q, q+1\})$

Theorem 1.5 *[11] (Truncation of groups in a transversal design) Let k be an integer, $k \geq 2$. Let $K = \{k, k+1, ..., k+s\}$. Suppose that there exists a $TD(k+s,m)$. Let $g_1, g_2, ...g_s$ be integers satisfying $0 \leq g_i \leq m, i = 1, 2, ..., s$. Then there exists a K-GDD of type $m^k g_1^1 \cdots g_s^1$.*

We also need a simple technique to establish nonexistence of PBDs:

Theorem 1.6 *[5] If a $PBD(v,K)$ contains a line of size h and another line of size k, and m is the smallest value in K, then $v \geq (m-1)h + k - m + 1$. Further, if the lines of size h and k are disjoint, then $v \geq (m-1)h + k$.*

2 An Update

In this section, we update the generating set for $\mathbb{Z}_{\geq 4}$, $\mathbb{Z}_{\geq 5}$ and $\mathbb{Z}_{\geq 6}$.

In [7], the following result is shown. Let $A_4 = [4,12] \cup [14,15] \cup [18,19]$ and $B_4 = \{23, 27\}$.

Theorem 2.1 *$A_4 \cup B_4$ is a generating set for $\mathbb{Z}_{\geq 4}$. Furthermore, the elements in A_4 are essential.*

Lemma 2.2 *$23 \notin B(A_4)$ and $27 \in B(A_4)$.*

Proof: If there exists a PBD$(23, A_4)$, then by Theorem 1.6 there must be no block of size greater than seven. Assume there exists a block of size seven. If there exists another block of size greater than five, then by Theorem 1.6, we obtain a contradiction. Applying Theorem 1.6, every block of size four or five must intersect the unique block of size seven. By removing the block of size seven, we obtain a PBD$(16, \{3,4\})$ so that the blocks partition into seven parallel classes. Simple counting shows that the 16 point PBD has exactly four blocks of size four, and hence has at most four parallel classes. Hence, it is impossible to have a block of size seven. If the PBD$(23, A_4)$ has only block of size four, five or six, then in [2] it was proved that it does not exist. Hence, $23 \notin B(A_4 \setminus \{23\})$. Finally, remove four points in an oval in a projective plane of order five to obtain $27 \in B(\{4,5,6\})$. □

As a consequence, we have the following theorem.

Theorem 2.3 *The minimal generating set for $\mathbb{Z}_{\geq 4}$ is $F_4 = [4,12] \cup [14,15] \cup [18,19] \cup \{23\}$.*

We now consider the generating set for $\mathbb{Z}_{\geq 5}$. In [7], Hanani proved the following theorem. Let $A_5 = [4,20] \cup [22,24]$ and $B_5 = [27,29] \cup [32,34] \cup \{39\}$.

Theorem 2.4 *$A_5 \cup B_5$ is a generating set for $\mathbb{Z}_{\geq 5}$ and the elements in the set A_5 are essential.*

In [10], $27, 28, 29$ were proved to be essential and 39 was proved to be in $B(\{5,6,7\})$.

Theorem 2.5 *The minimal generating set for $\mathbb{Z}_{\geq 5}$ is $F_5 = [4,20] \cup [22,24] \cup [27,29] \cup [32,34]$.*

Proof: We only need to show that $32, 33, 34 \notin B([5,31])$. If there is a block of size greater than eight, then the number of points is at least 37 by Theorem 1.6. If there is a block of size eight, then by Theorem 1.6 the number of points is at least 33. If $v = 33$, then we know from Theorem 1.6 that all other blocks must have size five. Removing the block of size eight gives a resolvable PBD with blocks of size four on 25 points, a contradiction. If $v = 34$, then by removing the unique block of size eight we obtain a $\{4,5,6\}$-PBD on 26 points. This must have a block of size six so the PBD$(34, \{5,6,7,8\})$ must have a block of size six disjoint from the block of size eight, or a block of size seven intersecting the block of size eight. In either case, it contradicts Theorem 1.6. So we must only show that $32, 33, 34 \notin PBD(\{5,6,7\})$. This is proved in [2]. □

We now consider $\mathbb{Z}_{\geq 6}$. In [7], the following result was proved. Let $A_6 = [6,30] \cup [32,36]$ and $B_6 = [37,41] \cup [45,47]$.

Theorem 2.6 *$A_6 \cup B_6$ is a generating set for $\mathbb{Z}_{\geq 6}$ and the elements in the set A_6 are essential.*

Let $F_6 = [6, 30] \cup [32, 41] \cup \{45\} \cup \{47\}$.

Theorem 2.7 *$F_6 \cup \{46\}$ is a generating set $\mathbb{Z}_{\geq 6}$ and the elements in the set F_6 are essential. Also, 46 is inessential if and only if the design $B(46, 6)$ exists.*

Proof: If a PBD$(v, (A_6 \cup B_6) \setminus \{v\})$, Theorem 1.6 shows that the design cannot contain a block of size greater than nine. If the design has a block of size nine, then $v \geq 46$. If $v = 46$, then every block must intersect the block of size nine and all other blocks must have size six. By removing the block of size nine, we have $37 \in B(5)$, a contradiction [7]. If $v = 47$, then every other block must intersect of size nine and the block must have size six or seven. By removing the block of size nine, we have $38 \in B(\{5, 6\})$, a contradiction [3]. Hence the largest block has size at most eight. In this case, the result follows from [2]. $\square$

3 $\mathbb{Z}_{\geq 7}$

In this section, we determine a generating set for $\mathbb{Z}_{\geq 7}$. The following result is very useful.

Let $E_{789} = [10, 48] \cup [51, 55] \cup [59, 62] \cup [93, 111] \cup [116, 118] \cup \{132\} \cup [138, 168] \cup [170, 216] \cup [219, 223] \cup [228, 230] \cup [242, 279] \cup [283, 286] \cup [298, 307] \cup [311, 342]$.

Theorem 3.1 *[9] For any $v \geq 7$, $v \in B(\{7, 8, 9\})$ except possibly when $v \in E_{789}$.*

We only need to consider elements of E_{789}.

Lemma 3.2 *If q is a prime power and $q \geq 11$, then $[7q + 24, q^2 + q] \in B([7, q + 1])$.*

Proof: Since q is a prime power, there exists a $TD(q + 1, q)$. For any integer $v \in [24, q^2 - 6q]$, it is possible to write v as a sum $g_1 + g_2 + \ldots + g_{q-6}$ where $q \geq g_i \geq 7$ or $g_i = 0$. The result follows by Theorem 1.5. $\square$

Lemma 3.3 $[92, 342] \in B([7, 19])$.

Proof: Apply Lemma 3.2 with $q = 11, 13, 16, 17, 19$. $\square$

Theorem 3.4 *The minimal generating set for $\mathbb{Z}_{\geq 7}$ is $F_7 = [7, 48] \cup [51, 55] \cup [59, 62]$.*

Proof: In view of Lemma 3.3, we only need to show that for any $v \in F_7$, $v \notin B(F_7 \setminus \{v\})$. Suppose to the contrary, $v \in B(F_7 \setminus \{v\})$. If the design contains a block of size greater than ten, Theorem 1.6 requires $v \geq 67$. If it has a block of size ten, then $v \geq 61$. If $v = 61$, all other blocks must have size 7 and must intersect the unique block of size ten. Removing the block of size ten yields a resolvable design on 51 points with block size six, but 51 is not a multiple of six, a contradiction. If $v = 62$, then all other blocks must have size seven or eight and must intersect the unique block of size ten. By removing the unique block of size ten, we obtain a PBD$(52, \{6,7\})$ whose blocks can be partitioned into ten parallel classes. Each parallel class must have type $6^4 7^4$. By counting unordered pairs, we must have $\frac{52(51)}{2} = 10(4\frac{6(5)}{2} + 4\frac{7(6)}{2})$. This gives $1326 = 1440$, a contradiction. Hence, there can not be a block of size greater than nine. So we have $v \in B(F_7 \setminus \{v\})$ if and only if $v \in B(\{7,8,9\})$. In [2], it was proved that $v \notin B(\{7,8,9\})$. $\Box$

4 $\mathbb{Z}_{\geq 8}$

In this section, we determine the minimal generating set for $\mathbb{Z}_{\geq 8}$.

Let $A_{8910} = [11,56] \cup [58,63] \cup [66,71] \cup [75,79]$ and $B_{8910} = [101,109] \cup [111,113] \cup [115,119] \cup [126,127] \cup [133,135] \cup [155,160] \cup [166,167] \cup [173,231] \cup \{239\} \cup [247,287] \cup [290,295] \cup [299,343] \cup [346,351] \cup [355,399] \cup [403,407] \cup [411,423] \cup [426,431] \cup [435,439] \cup [443,448] \cup [452,455] \cup [472,497] \cup [499,503] \cup [507,511] \cup [580,582]$.

Theorem 4.1 *[8] For any integer $v \geq 11$, $v \in B(\{8,9,10\})$ with the possible exceptions in B_{8910} and definite exceptions in A_{8910}.*

Lemma 4.2 $[101,133] \in B(\{8,9,10,11,12\})$.

Proof: Apply Theorem 1.4 with $q = 11$. $\Box$

Lemma 4.3 *If $q \geq 13$ and q is a prime power, then $[8q+24, q^2+q] \in B([8,q+1])$.*

Proof: For any integer $v \in [24, q^2 - 7q]$, v can be written as the sum of $g_1 + g_2 + \ldots + g_{q-7}$ where $8 \leq g_i \leq q$ or $g_i = 0$ for all $i = 1,2\ldots q-7$. Apply Theorem 1.5 with the existence of $TD(q+1,q)$. $\Box$

Lemma 4.4 $[128,582] \in B([8,25])$.

Proof: Apply Lemma 4.3 with $q = 13, 16, 17, 19, 23, 25$. $\Box$

Theorem 4.5 *The minimal generating set for $\mathbb{Z}_{\geq 8}$ is $F_8 = [8,56] \cup [58,63] \cup [66,71] \cup [75,79]$.*

Proof: In view of Lemmas 4.2 and 4.4, we only need to show for any $v \in F_8$, $v \notin B(F_8 \setminus \{v\})$. Suppose to the contrary, a PBD$(v, F_8 \setminus \{v\})$ design exists. If it contains a block of size $h \geq 12$, then Theorem 1.6 gives $v \geq 85$. If it has a block of size 11, then Theorem 1.6 requires $v \geq 78$. If $v = 78$, then every other block must have size eight and must intersect the block of size 11. By removing the block of size 11, we find $67 \in B(7)$, a contradiction [3]. If $v = 79$, then every other block must have size eight or nine and must intersect the block of size 11. By removing the block of size 11, we find $68 \in B(\{7,8\})$, a contradiction [3]. Hence, it cannot contain a block of size greater then 10. Theorem 4.1 completes the proof. $\Box$

5 $\mathbb{Z}_{\geq n}$

We first give an easy proof that $[n, 4n^2]$ is a generating set for $\mathbb{Z}_{\geq n}$.

Theorem 5.1 *$[n, 4n^2]$ is a generating set for $\mathbb{Z}_{\geq n}$.*

Proof: We prove the result inductively. If p_1 is a prime between $2n$ and $4n$, then by Theorem 1.5 we have $[np_1, p_1^2 + p_1 + 1] \in B([n, p_1 + 1])$. Note that $np_1 \leq n(4n)$ and $p_1 + 1 \leq 4n + 1 \leq 4n^2$. Hence, we have $[n, p_1^2 + p_1 + 1] \in B([n, p_1 + 1])$. Suppose we have p_k such that $[n, p_k^2 + p_k + 1] \in B([n, 4n^2])$ Let p_{k+1} be a prime such that p_{k+1} is between $p_k + 1$ and $2(p_k + 1)$. Clearly, $2(p_k + 1) \leq p_k^2 + p_k + 1$. Then $[np_{k+1}, p_{k+1}^2 + p_{k+1} + 1] \in B([n, p_{k+1} + 1]) \subseteq B([n, 4n^2])$. If we can check that $np_{k+1} \leq p_k^2 + p_k + 1$, then it follows that $[n, p_{k+1}^2 + p_{k+1} + 1] \in B([n, 4n^2])$ and the result follows by induction. But $np_{k+1} \leq 2n(p_k + 1) \leq p_1(p_k + 1) \leq p_k(p_k + 1) \leq p_k^2 + p_k + 1$. $\square$

Erdös and Larson [6] prove a much better result for sufficiently large values of n:

Theorem 5.2 *$[n, n^2 + f(n)]$ is a generating set for $\mathbb{Z}_{\geq n}$, where $f(n) = o(n^2)$.*

They use a variant of Theorem 1.4, and results on the differences between primes. We give another variant here:

Theorem 5.3 *Let n be a positive integer and $p > n$ be a prime power. Then $[n(p + 1), p^2 + p + 1] \subset B([n, p + 1])$.*

Proof: Since a projective plane of order p exists, $p^2 + p + 1 \in B(p + 1)$. If $np + n \leq v \leq (n + 2)(p - 1) - 1$, write $v - np = \alpha + \beta$, where $n \leq \alpha \leq p$ and $0 \leq \beta \leq p - n$. Apply Theorem 1.5 with $q = p$, $k = n$, $s = \beta + 1$, $g_1 = \cdots = g_\beta = 1$ and $g_{\beta+1} = \alpha$ to obtain $v \in B([n, p + 1])$.

Now let v satisfy $(n + 2)(p - 1) \leq v \leq p^2 + p$, and write $\widehat{v} = p^2 + p - v$ so that $0 \leq \widehat{v} \leq p^2 + p - (n + 2)(p - 1)$. If $\widehat{v} \leq (p - 1 - n)p + 2$, write $\widehat{v} = \alpha p + \beta + \gamma$, where $0 \leq \alpha \leq p - 2 - n$, $0 \leq \beta \leq p - n$, and $0 \leq \gamma \leq n + 2$. If $\widehat{v} > (p - 1 - n)p + 2$, instead choose $\alpha = p - 2 - n$, $\beta = p$ and $0 \leq \gamma \leq n + 2$.

Form a projective plane of order p containing an oval on $p + 1$ points. Delete a point of the oval to form a $TD(p + 1, p)$ with p groups $G_1, \ldots, G_p$ containing an oval point, and one group G_{p+1}; all groups have size p. Now delete all of the points in groups $G_{p+1}, \ldots, G_{p+2-\alpha}$ (when $\alpha = 0$, none are deleted.) Next delete β points from the group G_{n+3}. Finally delete just the oval point from α of the groups $G_1, \ldots, G_{n+2}$. The result is a PBD on v points with minimum block size n. $\square$

The consequences of Theorem 5.3 for particular values of n depend upon the distribution of primes and prime powers between $n+1$ and $2n$. In Table 1, a generating set for $\mathbb{Z}_{\geq n}$ consists of $[n, m(n) - 1]$ together with all numbers in the intervals listed in the "gaps". Naturally, for specific values of n, better results are possible, but this table gives a remarkably good starting point.

n	$m(n)$	Gaps
9	108	
10	120	134–139
11	154	184–186
12	168	184–203
13	221	
14	238	
15	255	
16	288	308–319,382–383
17	340	382–407
18	360	382–431
19	456	
20	480	
21	504	
22	528	554–571
23	598	
24	624	652–671
25	700	
26	728	758–779
27	810	
28	840	872–895,1058–1063
29	928	1058–1101
30	960	1058–1139
31	1023	1058–1177
32	1216	
33	1254	
34	1292	1408–1427
35	1330	1408–1469
36	1368	1408–1511
37	1554	
38	1596	
39	1638	
40	1680	1724–1759,1894–1919
41	1804	1894–1967
42	1848	1894–2015
43	2064	
44	2112	
45	2160	
46	2208	2258–2299,2452–2483
47	2350	2452–2537
48	2400	2452–2591,2864–2879
49	2646	2864–2939
50	2700	2864–2999
51	2754	2864–3059
52	2808	2864–3119
53	3180	
54	3240	
55	3300	
56	3360	
57	3420	
58	3480	3542–3595
59	3658	3784–3834
60	3720	3784–3899
61	3965	
62	4030	4162–4215
63	4095	4162–4283
64	4352	4558–4607
65	4420	4558–4679
66	4488	4558–4751
67	4824	
68	4896	5404–5439
69	4968	5404–5519
70	5040	5114–5179,5404–5599
71	5254	5404–5679
72	5328	5404–5759
73	5840	
74	5920	
75	6000	
76	6080	
77	6160	
78	6240	6322–6395,6974–7019
79	6478	6974–7109
80	6560	6644–6719,6974–7199
81	6804	6974–7289
82	6888	6974–7379,8012–8035
83	7470	8012–8133
84	7560	8012–8231
85	7650	8012–8329
86	7740	8012–8427
87	7830	8012–8525
88	7920	8012–8623
89	8722	
90	8820	
91	8918	
92	9016	
93	9114	
94	9212	9508–9587
95	9310	9508–9689
96	9408	9508–9791
97	9894	
98	9996	
99	10098	
100	10200	10304–10399,10714–10799

Figure 1: Consequences of Theorem 5.3

References

[1] R.J.R. Abel, A.E. Brouwer, C.J. Colbourn and J.H. Dinitz, Mutually Orthogonal Latin Squares (MOLS), in: *CRC Handbook of Combinatorial Designs*, to appear.

[2] L.M. Batten, Linear spaces with line range $\{n-1, n, n+1\}$ and at most n^2 points, *J. Austral. Math. Soc. (A)* 30 (1980), 215-228.

[3] F. Bennett, H.D.O.F. Gronau, A.C.H. Ling and R.C. Mullin, PBD-closure, in: *CRC Handbook of Combinatorial Designs*, to appear.

[4] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, England, 1986.

[5] D.A. Drake and J.A. Larson, Pairwise balanced designs whose lines sizes do not divide six, *J. Combin. Theory (A)* 34 (1983), 266-300.

[6] P. Erdös and J. Larson, On pairwise balanced block designs with the sizes of blocks as uniform as possible, *Ann. Discrete Math.* 15 (1982), 129-134.

[7] H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.* 11 (1975), 255-369.

[8] A.C.H. Ling and C.J. Colbourn, Pairwise balanced designs with block sizes 8,9 and 10, preprint.

[9] A.C.H. Ling, X.J. Zhu, C.J. Colbourn and R.C. Mullin, Pairwise balanced designs with consecutive block sizes, preprint.

[10] Y. Miao, A note on a generating set for N_5, *J. Combin. Math. and Combin. Computing* 15 (1994), 227-228.

[11] R.C. Mullin and H.D.O.F. Gronau, PBDs: Recursive Constructions, in: *CRC Handbook of Combinatorial Designs*, to appear.