

# On bipartite biregular large graphs derived from difference sets\*

G. Araujo-Pardo<sup>a</sup>, C. Dalfó<sup>b</sup>, M. A. Fiol<sup>c</sup>, N. López<sup>d</sup>

<sup>a</sup>Instituto de Matemáticas, Universidad Nacional Autónoma de México,  
Mexico, [garaujo@math.unam.mx](mailto:garaujo@math.unam.mx)

<sup>b</sup>Departament de Matemàtica, Universitat de Lleida,  
Igualada (Barcelona), Catalonia, [cristina.dalfo@udl.cat](mailto:cristina.dalfo@udl.cat)

<sup>c</sup>Departament de Matemàtiques, Universitat Politècnica de Catalunya,  
Barcelona Graduate School of Mathematics,  
Institut de Matemàtiques de la UPC-BarcelonaTech (IMTech)

Barcelona, Catalonia, [miguel.angel.fiol@upc.edu](mailto:miguel.angel.fiol@upc.edu)

<sup>d</sup> Departament de Matemàtica, Universitat de Lleida,  
Lleida, Spain, [nacho.lopez@udl.cat](mailto:nacho.lopez@udl.cat)

## Abstract

A bipartite graph  $G = (V, E)$  with  $V = V_1 \cup V_2$  is biregular if all the vertices of each stable set,  $V_1$  and  $V_2$ , have the same degree,  $r$  and  $s$ , respectively. This paper studies difference sets derived from both Abelian and non-Abelian groups. From them, we propose some constructions of bipartite biregular graphs with diameter  $d = 3$  and asymptotically optimal order for given degrees  $r$  and  $s$ . Moreover, we find some biMoore graphs, that is, bipartite biregular graphs that attain the Moore bound.

---

\*The research of the G. Araujo-Pardo is supported by PAPIIT-México under Project IN101821 and Proyecto de Intercambio Académico 1926: “Gráficas de Moore, Jaulas, Diseños de Bloques y Número Cromático”, CIC-UNAM. The research of C. Dalfó, M. A. Fiol, and N. López has been supported by AGAUR from the Catalan Government under project 2021SGR00434 and MICINN from the Spanish Government under project PID2020-115442RB-I00. The research of M. A. Fiol was also supported by a grant from the Universitat Politècnica de Catalunya with references AGRUPS-2022 and AGRUPS-2023.

*Keywords:* Bipartite biregular graphs, Moore bound, diameter, adjacency spectrum.

*MSC2020:* 05C35, 05C50.

## 1 Introduction

The *degree/diameter problem* for graphs is finding the largest order of a graph with the prescribed degree and diameter. The maximum of this number is the *Moore bound*, and a graph whose order coincides with this bound is called a *Moore graph*. There is much work related to this topic (see the survey by Miller and Širáň [8]), and also to this subject with some restrictions of the original problem. One of them is related to the bipartite Moore graphs. In this case, the goal is to find regular bipartite graphs with maximum order and fixed diameter. In this paper, we deal with the problem initiated by Yebra, Fiol, and Fàbrega [10] in 1983, which consists of finding biregular bipartite Moore graphs.

A bipartite graph  $G = (V, E)$  with  $V = V_1 \cup V_2$  is *biregular* if all the vertices of the stable set  $V_i$ , for  $i = 1, 2$ , have the same degree. We denote  $[r, s; d]$ -bigraph a bipartite biregular graph of degrees  $r$  and  $s$  and diameter  $d$ ; and by  $[r, s; d]$ -biMoore graph the bipartite biregular graph of diameter  $d$  that attains the Moore bound, which is denoted  $M(r, s; d)$ . Notice that constructing these graphs is equivalent to constructing block designs, where one partite set corresponds to the points of the block design, and the other set corresponds to the blocks of the design. Moreover, each point is in a fixed number  $s$  of blocks, and each block's size equals  $r$ . The incidence graph of this block design is an  $[r, s; d]$ -bigraph.

We propose some constructions of bipartite biregular graphs with diameter  $d = 3$  and asymptotically optimal order for given degrees  $r$  and  $s$ . Our main tool is the use of difference sets. The same approach was used by Erskine, Fratrič, and Širáň [4], where they employed perfect difference sets to obtain graphs with diameter two and asymptotically optimal order for their maximum degree. Moreover, they proved that their graphs were isomorphic to some of the Brown graphs [2], a well-known family of graphs in the degree/diameter problem.

This paper is structured as follows. The following subsection gives the Moore-like bound for bipartite biregular graphs with an odd diameter. In Subsection 1.2, we give a new improved Moore bound for diameter 3. In Section 2, we study the bipartite biregular graphs derived from difference sets of Abelian groups. We give the so-called covering difference sets for  $s = 7$  in Section 3. Finally, in Subsection 3.1, we deal with a bipartite biregular graph derived from difference sets of non-Abelian groups.

## 1.1 Moore-like bounds

Let  $G = (V, E)$ , with  $V = V_1 \cup V_2$ , be an  $[r, s; d]$ -bigraph, where each vertex of  $V_1$  has degree  $r$ , and each vertex of  $V_2$  has degree  $s$ . Let  $N_i = |V_i|$  for  $i = 1, 2$ . Then, counting in two ways the number of edges of  $G$ , we have  $rN_1 = sN_2$ . Moreover, if the diameter is odd, say,  $d = 2m + 1$  (for  $m \geq 1$ ), and  $u \in V_1$ , we have (from the number of vertices at distance  $0, 1, 2, \dots, d - 1$  from  $u$ ):

$$N_1 \leq 1 + r(s - 1) \frac{[(r - 1)(s - 1)]^m - 1}{(r - 1)(s - 1) - 1} = N'_1, \quad (1)$$

whereas, if  $u \in V_2$  (interchanging  $r$  and  $s$ ):

$$N_2 \leq 1 + s(r - 1) \frac{[(r - 1)(s - 1)]^m - 1}{(r - 1)(s - 1) - 1} = N'_2. \quad (2)$$

Since  $N'_1 r \neq N'_2 s$ , the Moore bound must be smaller than  $N'_1 + N'_2$ . It was proved in Yebra, Fiol, and Fàbrega [10] that, assuming  $r > s$ ,

$$N_1 \leq \left\lfloor \frac{N'_1}{\rho} \right\rfloor \sigma \quad \text{and} \quad N_2 \leq \left\lfloor \frac{N'_2}{\rho} \right\rfloor \rho, \quad (3)$$

where  $\rho = \frac{r}{\gcd\{r, s\}}$  and  $\sigma = \frac{s}{\gcd\{r, s\}}$ . Thus, the Moore bound for odd diameter  $d = 2m + 1$  is

$$M(r, s; 2m + 1) = \left\lfloor \frac{1 + s(r - 1) \frac{[(r - 1)(s - 1)]^m - 1}{(r - 1)(s - 1) - 1}}{\rho} \right\rfloor (\rho + \sigma). \quad (4)$$

For diameter  $d = 3$  ( $m = 1$ ), the Moore bounds in (4) become

$$M(r, s; 3) = \left\lfloor \frac{1 + s(r - 1)}{\rho} \right\rfloor (\rho + \sigma), \quad (5)$$

with  $\rho = \frac{r}{\gcd\{r, s\}}$  and  $\sigma = \frac{s}{\gcd\{r, s\}}$ .

Two bipartite biregular graphs with diameter three attaining the Moore bound (5) were given in Yebra, Fiol, and Fàbrega [10]. Namely, in Figure 1(a), with  $r = 4$  and  $s = 3$ , we would have the unattainable values  $(N'_1, N'_2) = (9, 10)$ , whereas we get  $(N_1, N_2) = (6, 8)$ , giving  $M(4, 3; 3) = 14$ . In Figure 1(b), with  $r = 5$  and  $s = 3$ , we have  $(N'_1, N'_2) = (11, 13)$ , and  $(N_1, N_2) = (6, 10)$ , now corresponding to  $M(5, 3; 3) = 16$ . In Figure 1(c), with  $r = 6$  and  $s = 3$ , there is an optimal (unique)  $[6, 3; 3]$ -bigraph on 21 vertices, whereas the Moore bound is  $M(6, 3; 3) = 8 + 16 = 24$ .

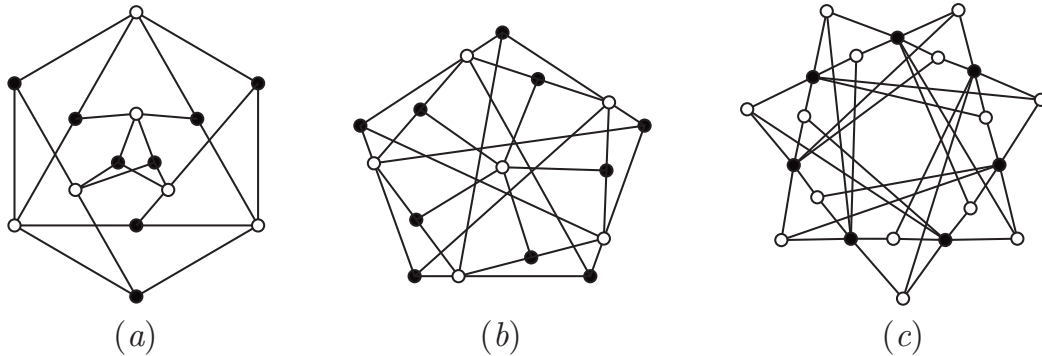


Figure 1: (a) The only  $[4,3;3]$ -biMoore graph on 14 vertices; (b) One of the two  $[5,3;3]$ -biMoore graphs on 16 vertices; (c) The only  $[6,3;3]$ -biMoore graph on 21 vertices.

In [1], the authors studied the simple case of biMoore graphs with degrees  $r$  (even),  $s = 2$ , and diameter  $d \leq 3$ . For these values, the Moore bounds in (5) turn out to be  $M(r, 2; 3) = 2 + r$  when  $r(> 1)$  is odd, attained by the complete bipartite graph  $K_{r,2}$  with  $d = 2$ , and  $M(r, 2; 3) = 3(1 + \frac{r}{2})$  when  $r(> 2)$  is even. In the last case, the bound is obtained by a graph with three vertices,  $u_1, u_2, u_3$ , where each pair  $(u_i, u_j)$  is joined by  $r$  paths of length 2. In the same paper, a numeric construction of bipartite biregular Moore graphs for diameter  $d = 3$  and degrees  $r$  and  $s = 3$  was proposed.

In general, and in terms of designs, to guarantee that the diameter equals 3, any pair of points must share a block, and any pair of blocks must have a non-empty intersection. It is well known that this kind of structure exists when  $r = m$  and  $r - 1$  is a prime power. Namely, the so-called projective plane of order  $r - 1$ . In this case, any pair of blocks (or lines) intersect in exactly one point and, for any pair of points, they share one and only one block (or line). For more details about projective planes, you can consult, for instance, Coxeter [3]. This condition is unnecessary in our constructions of block designs, which give graphs of diameter of 3. Two blocks can be intersected in more than one point, and two points can share one or more blocks. Moreover, we may have the same block appearing more than once. In the following section, we construct graphs with orders that attain or are close to such Moore bounds.

## 1.2 An improved Moore bound for diameter 3

In this subsection, we prove that, for diameter 3 and some values of the degrees  $r$  and  $s$ , the Moore bound in (5) can be improved. We begin with the case  $r = s^2$ .

$r \setminus s$	2	3	4	5	6	7	8	9	10	11	12
2	<sup>(6)</sup> <b>6</b>										
3	-	<sup>(14)</sup> <b>14</b>									
4	<sup>(9)</sup> <b>9</b>	<sup>(14)</sup> <b>14</b> <sup>*◇</sup>	<sup>(26)</sup> <b>26</b>								
5	-	<sup>(16)</sup> <b>16</b> <sup>*</sup>	27	<sup>(42)</sup> <b>42</b>							
6	<sup>(12)</sup> <b>12</b>	<sup>(24)</sup> <b>21</b> <sup>◇</sup>	<sup>(35)</sup> 30	44	<sup>(62)</sup> <b>62</b>						
7	-	<sup>(20)</sup> <b>20</b> <sup>*</sup>	33	48	65	86					
8	<sup>(15)</sup> <b>15</b>	<sup>(22)</sup> <b>22</b> <sup>*</sup>	42	52	70	90	<sup>(114)</sup> <b>114</b>				
9	-	<sup>(32)</sup> <b>28</b> <sup>*</sup>	39	56	80	96	119	<b>146</b>			
10	<sup>(18)</sup> <b>18</b>	<sup>(26)</sup> <b>26</b> <sup>*</sup>	49	<sup>(69)</sup> 66	<sup>(88)</sup> 80	102	126	152	<sup>(182)</sup> <b>182</b>		
11	-	<sup>(28)</sup> <b>28</b> <sup>*</sup>	45	64	85	108	133	160	189	222	
12	<sup>(21)</sup> <b>21</b>	<sup>(40)</sup> <b>35</b> <sup>*</sup>	60	68	99	114	145	175	198	230	<sup>(266)</sup> <b>266</b>

Table 1: Moore bounds (5) for diameter  $d = 3$  (between parenthesis when a better or optimal construction is known). The known optimal values (most coinciding with the Moore bound) are in boldface. The asterisks correspond to the graphs obtained in [1] (see also Proposition 2.2 of that paper), and the diamonds correspond to unique graphs. The cases when  $r = s = q + 1$ , with  $q$  a prime power, correspond to the point-line incidence graphs of the projective planes.

**Lemma 1.1.** *Let  $G = (V_1 \cup V_2, E)$  be an  $[r, s; 3]$ -bigraph, with  $r \geq s$ , such that  $N_2 = s(r - 1)$ . Then, the following conditions hold:*

- (i) *Either  $r = s$  or  $r = s^2$ .*
- (ii) *For any  $u \in V_2$ , there exists a unique vertex namely  $r(u) \in V_2$  (the repeat of  $u$ ) such that  $|N(u) \cap N(r(u))| = 2$ , where  $N(u)$  is the set of vertices that are neighbors of  $u$  (at distance 1).*

*Proof.* (i) From  $rN_1 = sN_2$  and assuming  $N_2 = s(r - 1)$ , we have  $N_1 = \frac{s^2(r-1)}{r}$ . Besides,  $\gcd(r, r - 1) = 1$  and, as a consequence,  $r$  must divide  $s^2$ . Since  $r \geq s$ , the

only possibilities are either  $r = s$  or  $r = s^2$ .

(ii) Now, we prove that, for any  $u \in V_2$ , there exists a unique vertex, namely,  $r(u) \in V_2$  (the *repeat* of  $u$ ) such that  $|N(u) \cap N(r(u))| = 2$ . There are exactly two different paths from  $u$  to  $r(u)$  of length 2. Indeed, since the diameter of  $G$  is three, for every  $u' \in V_2$ , with  $u' \neq u$ ,  $\text{dist}(u, u') = 2$  must hold. The maximum number of vertices at distance 2 from  $u$ , allowed by the vertex degrees, is  $s(r - 1)$  and since  $N_2 = s(r - 1)$  by hypothesis. Then, the existence of a vertex  $r(u)$  sharing two neighbors with  $u$  is guaranteed. Moreover, for the remaining vertices  $u'$  of  $V_2$ , others than  $r(u)$ , there must be a unique path of length 2 from  $u$  to  $u'$ .  $\square$

The case  $r = s^2$  is very interesting since the condition  $N_2 = s(r - 1)$  provides the Moore bound in (5). In fact, as a consequence of Lemma 1.1, such a bound can be improved.

**Proposition 1.2.** *Given  $s \geq 3$ , there is no  $[s^2, s; 3]$ -bigraph with order attaining the Moore bound in (5),  $M(s^2, s; 3) = (s^2 - 1) + (s^3 - s)$ . Instead, the new, improved Moore bound is*

$$M^*(s^2, s; 3) = (s^2 - 2)(s + 1), \quad (6)$$

obtained with

$$N_1 = s^2 - 2 \quad \text{and} \quad N_2 = s^3 - 2s. \quad (7)$$

*Proof.* Assume that  $M(s^2, s; 3)$  is attained and, hence,  $N_1 = s^2 - 1$  and  $N_2 = s^3 - s$ . Then, we claim that, for any  $v \in V_1$ , there exists another vertex  $v' \in V_1$  such that  $|N(v) \cap N(v')| \geq 3$ . Indeed, assume to the contrary that  $|N(v) \cap N(w)| \leq 2$  for all  $w \in V_1$ , with  $w \neq v$ . Then, the number of edges from  $V_1 \setminus \{v\}$  to  $N(v)$  would be  $\leq 2(N_1 - 1)$ . Moreover,  $|N(v)| = s^2$  and, since every vertex in  $N(v)$  has degree  $s$ , the number of edges from  $N(v)$  to  $N^2(v) (= V_1 \setminus \{v\})$  is  $s^2(s - 1)$ , where  $N^2(v)$  is the set of vertices at distance 2 from  $v$ . As a consequence,  $s^2(s - 1) \leq 2(N_1 - 1)$ . Hence,  $N_1 \geq \frac{1}{2}s^2(s - 1) + 1$ , which, for  $s \geq 3$ , is greater than  $s^2 - 1$ , a contradiction. Thus, for any  $v \in V_1$ , there exists another vertex  $v' \in V_1$  such that  $|N(v) \cap N(v')| \geq 3$ . Let  $N(v) \cap N(v') = \{u_1, u_2, \dots, u_l\} \subset V_2$ , where  $l \geq 3$ . Notice that every  $u_i$ , with  $i = 2, \dots, l$ , is a repeated vertex of  $u_1$  since there are two different paths  $u_1 - v - u_i$  and  $u_1 - v' - u_i$  joining them, but this is a contradiction with the fact that there is a unique repeated vertex for any vertex in  $V_2$ , as we proved in Lemma 1.1. Therefore, our initial assumption is false, and the new possible values of  $N_1$  and  $N_2$  satisfying  $s^2N_1 = sN_2$  are those in (7).  $\square$

The above proposition can be generalized to give an improved Moore bound for  $[\rho s, s; 3]$ -bigraphs under some conditions on  $\rho$  and  $s$ . With this aim, we extend the concept of repeat to *redundant paths*, defined as expected: The number of redundant

$s \setminus r$	6	9	12	16	20	24	25	28	30	32	35	36
3	<b>21</b>	<b>28</b>										
4	-	-	56	70	84	98	-	112	-	126	-	140
5	-	-	-	-	115	-	138	-	161	-	184	-

Table 2: Improved Moore bounds (8) for diameter  $d = 3$ . The known optimal values are in boldface. (Compare with the values in Table 1.)

paths between a vertex  $u$  to a vertex subset  $U$  is the total number of shortest paths from  $u$  to  $U$  minus  $|U|$ .

**Proposition 1.3.** *Given  $s \geq 3$  and  $\rho$  such that  $s - 1 \leq \rho \leq s^2 - s - 3$ , there is no  $[\rho s, s; 3]$ -bigraph with order attaining the Moore bound in (5),  $M(\rho s, s; 3) = (s^2 - 1)(\rho + 1)$ . Instead, the new, improved Moore bound is*

$$M^*(\rho s, s; 3) = (s^2 - 2)(\rho + 1), \quad (8)$$

obtained with

$$N_1 = s^2 - 2 \quad \text{and} \quad N_2 = \rho(s^2 - 2). \quad (9)$$

*Proof.* Suppose that, by contradiction, the bound  $M(\rho s, s; 3)$  with  $N_1 = s^2 - 1$  and  $N_2 = \rho(s^2 - 1)$  is attained. Then, the number of redundant 2-paths from  $u \in V_2$  to  $V_2 \setminus \{u\}$  is

$$s(r - 1) - (N_2 - 1) = s(\rho s - 1) - \rho(s^2 - 1) + 1 = \rho - s + 1.$$

Then, we claim that, for any  $v \in V_1$ , there exists another vertex  $v' \in V_1$  such that  $|N(v) \cap N(v')| \geq \rho - s + 3$ . If not, we would have that  $|N(v) \cap N(w)| \leq \rho - s + 2$  for all  $w \in V_1$ , with  $w \neq v$ . Hence, the number  $e = \rho s(s - 1)$  of edges from  $V_1 \setminus \{v\}$  to  $N(v)$  would be at most  $(\rho - s + 2)(N_1 - 1)$ . As a consequence, from  $\rho s(s - 1) \leq (\rho - s + 2)(N_1 - 1)$ , we would have that  $N_1 \geq \frac{\rho s(s-1)}{\rho-s+2}$ . However, the function

$$\phi(\rho, s) = \frac{\rho s(s - 1)}{\rho - s + 2} - (s^2 - 1)$$

is positive for  $s \geq 3$  and  $s - 2 < \rho < s^2 - s - 2$  (see Figure 2), a contradiction. Thus, for any  $v \in V_1$ , there exists another vertex  $v' \in V_1$  such that  $|N(v) \cap N(v')| \geq \rho - s + 3$ . From here, we reason as in the proof of Proposition 1.2 to conclude (8).  $\square$

See some examples of these improved new values of the Moore bound in Table 2, for  $s = 3, 4$ , and  $5$ .

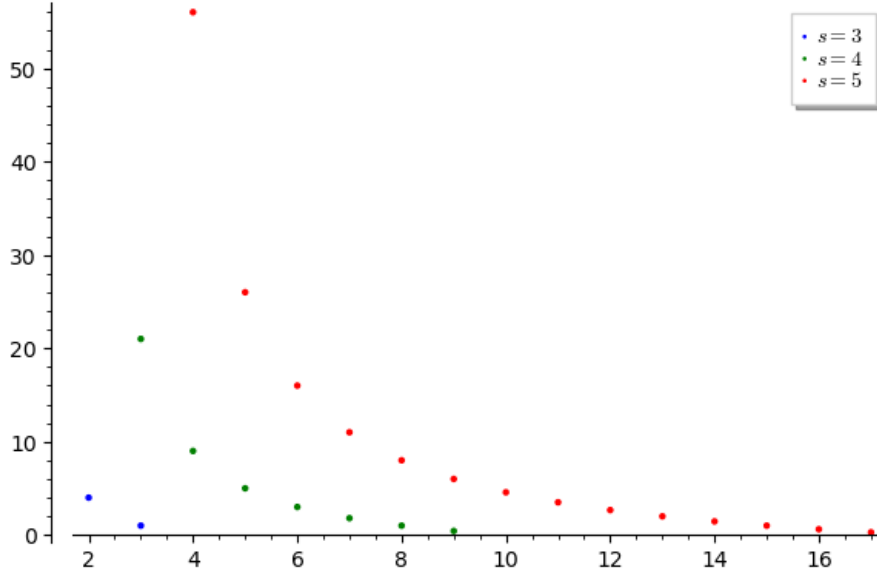


Figure 2: The values of the function  $\phi(\rho, s)$  for  $s = 3$  (blue),  $s = 4$  (green) and  $s = 5$  (red).

## 2 Bipartite biregular graphs derived from difference sets

Given a group  $(\Gamma, \cdot)$  of order  $n$ , an  $(n, s, \lambda)$ -difference set in  $\Gamma$  is an  $s$ -subset  $S$  of  $\Gamma$  such that each non-identity element  $g \in \Gamma$  occurs exactly  $\lambda$  times in the multiset  $\{t_i \cdot t_j^{-1} \mid t_i, t_j \in S\}$ . The study of the difference sets of groups dates back to the thirties of the past century (see Singer [9]). His study is focused mainly on the difference sets of Abelian groups, where the additive notation  $\{t_i - t_j \mid t_i, t_j \in S\}$  is commonly used. In particular, a difference set with  $\lambda = 1$  is called *perfect*. For instance, in the case of  $\Gamma = \mathbb{Z}_{13}$ , we can take  $S = \{0, 1, 3, 9\}$ . As shown in the following table, here in additive notation,  $d_{ij} = i - j \pmod{13}$  for  $i, j \in S$ , the *difference matrix*  $\mathbf{D}_S = (d_{ij})$  gives each non-zero residue modulo 13 exactly once. That is,  $S$  is a  $(13, 4, 1)$ -difference set.

$i \setminus j$	0	1	3	9
0	0	12	10	4
1	1	0	11	5
3	3	2	0	7
9	9	8	6	0

$$, \quad \mathbf{D}_S = \begin{pmatrix} 0 & 12 & 10 & 4 \\ 1 & 0 & 11 & 5 \\ 3 & 2 & 0 & 7 \\ 9 & 8 & 6 & 0 \end{pmatrix}.$$

Let  $S$  be a subset of cardinality  $s$  of a given group  $\Gamma$  of order  $n$ . We say that  $S$  is a *covering difference set* of  $\Gamma$  if the multiset of differences  $\{t_i \cdot t_j^{-1} \mid t_i, t_j \in S\}$  contains all the elements of  $\Gamma$  (perhaps with some repetitions). That is, the difference matrix

$\mathbf{D}_S$  covers all the elements of  $\Gamma$ . We use these sets to construct bipartite biregular graphs with large order as follows.

**Definition 2.1.** *Given  $\Gamma$  and  $S$  as above, and an integer  $m \geq 1$ , let  $G_m(S) = (V_0 \cup V_1, E)$  be the bipartite graph with independent sets  $V_0 = \{(0, u) : u \in \Gamma\}$ ,  $V_1 = \{(l, v) : v \in \Gamma \text{ and } 1 \leq l \leq m\}$ , and adjacencies  $(l, v) \sim (0, v \cdot \sigma)$  for all  $\sigma \in S$  and  $l \in \{1, \dots, m\}$ .*

The next result gives the main properties of these graphs.

**Proposition 2.2.** *Let  $\Gamma$  be an Abelian group with  $n$  elements and a covering  $s$ -set  $S$ . Then, the bipartite graph  $G_m(S)$  has  $(m + 1)n$  vertices, where every vertex in  $V_0$  has degree  $s$  and every vertex in  $V_1$  has degree  $ms$ . Moreover, the diameter of  $G_m(S)$  is 3.*

*Proof.* The order of  $G_m(S)$  follows directly from the definition:  $V_0$  contain the  $n$  elements of  $\Gamma$ , meanwhile  $V_1$  contains  $m$  different copies of  $\Gamma$ . Let  $S = \{t_1, \dots, t_s\}$ . Notice that each vertex  $(j, v) \in V_1$  is adjacent to  $(0, v \cdot t_1), (0, v \cdot t_2), \dots, (0, v \cdot t_s)$  and all these vertices are different since  $\Gamma$  is a group. Besides, each vertex of  $V_2$ , say  $(0, v)$ , is adjacent to  $(l, v \cdot t_i^{-1})$  for all  $1 \leq l \leq m$  and  $t_i \in S$ . This gives the desired degrees. To see that the diameter is 3, it suffices to prove that every pair of different vertices  $(0, u), (0, u') \in V_1$ , and every pair of different vertices  $(l, v), (l', v') \in V_1$ , are at distance two.

In the second case, we have the following path of length 2:

$$(l, v) \sim (0, v \cdot t_i) \sim (l', v \cdot t_i \cdot t_j^{-1}) \quad \text{for all } t_i, t_j \in S \text{ and } l, l' \in \{1, \dots, m\}.$$

Notice that  $t_i \cdot t_j^{-1}$  is precisely the element  $d_{ij}$  in the difference matrix  $\mathbf{D}_S$  and, hence, it provides every element of  $\Gamma$  under the hypothesis. A path of length 2 between vertices in  $V_0$  is given by:

$$(0, v) \sim (l, v \cdot t_i^{-1}) \sim (0, v \cdot t_i^{-1} \cdot t_j) \quad \text{for all } t_i, t_j \in S \text{ and } l \in \{1, \dots, m\}. \quad (10)$$

Since  $\Gamma$  is an Abelian group, then  $t_i^{-1} \cdot t_j = t_j \cdot t_i^{-1}$ , and so every element in  $\Gamma$  can be represented as  $v \cdot t_i^{-1} \cdot t_j$  by the hypothesis.  $\square$

For example, in Figure 3, there is the graph  $G_2(S)$  obtained from the perfect set  $S = \{0, 1, 3\}$  in  $\Gamma = \mathbb{Z}_7$ . It has 21 vertices, degrees  $(6, 3)$ , and diameter  $d = 3$ . Although the corresponding Moore bound is 24, this graph is known to be optimal. In fact,  $S$  is a perfect difference set from where the best results are obtained. Another example is the graph  $G_2(S)$  of Figure 4, where  $S = \{0, 1, 3, 9\}$  is the perfect difference

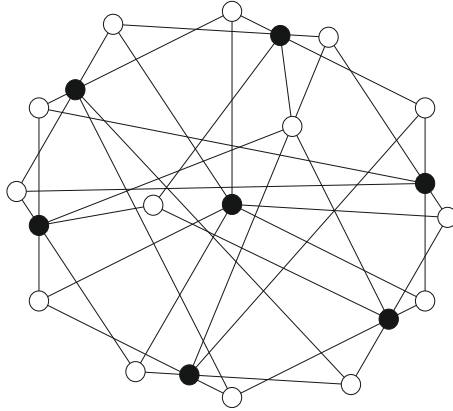


Figure 3: The graph  $G_2(\{0, 1, 3\})$  over  $\mathbb{Z}_7$ . It has 21 vertices, degrees  $(6, 3)$  and diameter 3.

set on  $\mathbb{Z}_{13}$  shown at the beginning of this section. Then, it has 39 vertices, degrees  $(8, 4)$ , and diameter 3.

A simple counting argument says that any  $(n, s, \lambda)$ -difference set  $S$  must satisfy  $\lambda(n-1) = s(s-1)$ . Given an  $s$ -subset  $S$ , the equality  $n = s^2 - s + 1$  must hold to look for a perfect difference set in a group  $\Gamma$  of order  $n$ .

Then, it is known that, for every prime power  $q$ , there exists a perfect  $(n, s, 1)$ -difference set  $S$  with  $s = |S| = 1 + q$  elements, and  $n = q^2 + q + 1 = s^2 - s + 1$  (see Singer [9], and Halberstam and Laxton [7]). In fact, Singer proved that if  $S = \{s_i : 0 \leq i \leq q\}$  is a perfect difference set modulo  $n = q^2 + q + 1$ , and if lines  $L_i$  and points  $P_j$  (for  $i, j \in \mathbb{Z}_n$ ) of  $S$  are defined in such a way that each line  $L_i$  contains the set of points  $P_j = i + s_j$  for  $j = 0, 1, \dots, q$ , then  $S$  is a projective plane. As a consequence, the graphs  $G_1(S)$  of Proposition 2.2 with  $r = s = q + 1$  turn out to be the point-line incidence graphs of the projective planes  $PG(2, q)$ .

A handy way of obtaining a difference set  $S$  with  $s = |S| = q + 1$  elements, relative to the group  $\mathbb{Z}_n$  with  $n = q^2 + q + 1$ , is as follows. Let  $\phi(x)$  be a polynomial of degree 3, with coefficients in  $GF(q) \cong \mathbb{Z}_q$ , irreducible (so that  $\phi(\alpha) \neq 0 \pmod{q}$  for every  $\alpha \in GF(q)$ ) and primitive (so that  $r = q^n - 1$  is the smallest integer such that  $\phi(x)$  divides  $x^r - 1$ ). Then, in the extension field  $F = GF(q^3)$  of polynomials mod  $\phi(x)$ , the monic polynomial  $x$  is primitive. Hence, the elements of the multiplicative (cyclic) group  $F^*$  of  $GF(q^3)$  can be represented as the powers  $x^0 = 1, x^1 = x, x^2, \dots, x^{r-1} \pmod{\phi(x)}$ . Now, suppose that, in  $F$ , the elements  $1 + x, 1 + 2x, \dots, 1 + (q-1)x$  correspond to  $x^{s_1}, x^{s_2}, \dots, x^{s_{q-1}}$ , respectively. Then, the set  $S = \{0, 1, s_1, s_2, \dots, s_{q-1}\}$  is a difference set with  $q + 1$  elements, relative to  $\mathbb{Z}_{q^2+q+1}$ . (Of course, all the numbers  $s_i$ , for  $i = 1, 2, \dots, q - 1$ , can be reduced modulo  $m$  so that  $2 \leq s_i \leq n - 1$ ). For

example, if  $q = 3$ , a primitive polynomial to derive the extension field  $F = GF(3^3)$  is  $\phi(x) = x^3 + 2x^2 + x + 1$ . Then, the elements of  $F$  are:

$$\begin{array}{llll}
x^0 = 1, & x^1 = x & x^2 = x^2 & x^3 = x^2 + 2x + 2 \\
x^4 = x + 2, & x^5 = x^2 + 2x, & x^6 = 2x + 2, & x^7 = 2x^2 + 2x, \\
x^8 = x^2 + x + 1, & x^9 = 2x^2 + 2 & x^{10} = 2x^2 + 1, & x^{11} = 2x^2 + 2x + 1 \\
x^{12} = x^2 + 2x + 1, & x^{13} = 2, & x^{14} = 2x, & x^{15} = 2x^2, \\
x^{16} = 2x^2 + x + 1, & \mathbf{x^{17} = 2x + 1}, & x^{18} = 2x^2 + x, & \mathbf{x^{19} = x + 1}, \\
x^{20} = x^2 + x, & x^{21} = 2x^2 + 2x + 2, & x^{22} = x^2 + 1, & x^{23} = x^2 + 2, \\
x^{24} = x^2 + x + 2, & x^{25} = 2x^2 + x + 2. & & 
\end{array}$$

Therefore, a difference set for  $\mathbb{Z}_n$ , with  $n = q^2 + q + 1 = 13$ , is  $S = \{0, 1, 17, 19 \pmod{13}\} = \{0, 1, 4, 6\}$  (see the table below).

$i \setminus j$	0	1	4	6
0	0	12	9	7
1	1	0	10	8
4	4	3	0	11
6	6	5	2	0

We get the following consequence from Proposition 2.2.

**Corollary 2.3.** *Let  $s = 1 + q$  with  $q$  a prime power. Let  $n = s^2 - s + 1$ . Then, for every  $m \geq 1$ , there is a bipartite graph  $G_m(S)$  on  $(m + 1)n$  vertices and degrees  $r = ms$  and  $s$  with diameter  $d = 3$ .*

Thus, these graphs  $G_m(S)$ , with pair of degrees  $(ms, s)$ , have order

$$|V_0| + |V_1| = n(m + 1) = (s^2 - s + 1)(m + 1), \quad (11)$$

whereas, the Moore bound (5) for degrees  $(r, s) = (ms, s)$  and diameter 3 is

$$M(ms, s; 3) = (m + 1) \left\lfloor s^2 - \frac{s - 1}{m} \right\rfloor = (s^2 - 1)(m + 1) \quad (12)$$

when  $m \geq s + 1$ , and the improved Moore bound (8) is

$$M^*(ms, s; 3) = (s^2 - 2)(m + 1) \quad (13)$$

when  $s - 1 \leq m \leq s^2 - s - 3$ . So, whenever the graphs are in the setting of Corollary 2.3, their order asymptotically approaches the Moore bound (12) of diameter 3 with the ratio

$$\gamma = \frac{s^2 - s + 1}{s^2 - 1}.$$

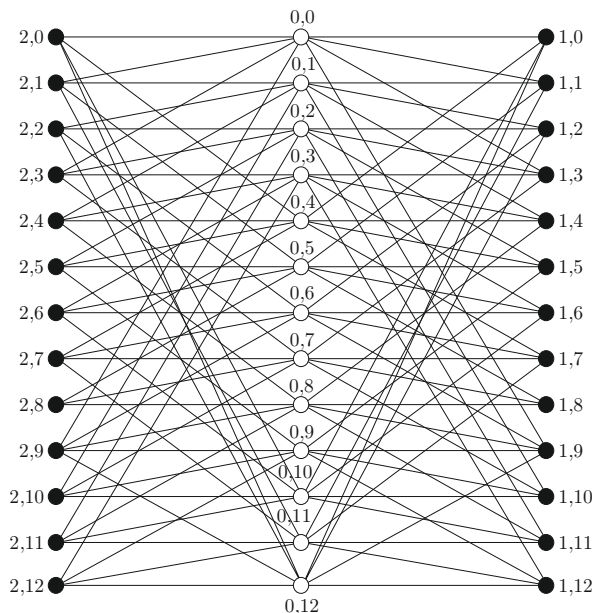


Figure 4: The bipartite graph  $G_2(\{0, 1, 3, 9\})$  over  $\mathbb{Z}_{13}$ . It has 39 vertices, degrees  $(8, 4)$ , and diameter 3.

In particular, when  $s - 1 \leq m \leq s^2 - s - 3$ , the values in (11) and (13) coincide, and we get  $(3m, 3; 3)$ -biMoore graphs. In Table 3, we show perfect difference sets for  $s \leq 12$ , together with the parameters of the corresponding graphs  $G_m(S)$  and the improved Moore bound (8) provided that  $s - 1 \leq m \leq s^2 - s - 3$  (otherwise, we must use (5)). For instance, the family of graphs  $G_m(S)$ , constructed with the  $(13, 4, 1)$ -difference set  $S = \{0, 1, 3, 9\}$ , produces a bipartite graph with degrees  $r = 4m$  and  $s = 4$  having  $13(m + 1)$  vertices and diameter  $d = 3$ .

The corresponding Moore bound for this case  $(4m, 4; 3)$  is 42 for  $m = 2$ , and  $15(m + 1)$  for  $m \geq 3$ . As a consequence, the family of graphs  $G_m(S)$  asymptotically approaches the Moore bound with a constant ratio of  $\frac{13}{15} \approx 0.867$ . In particular, for  $m = 2$ , the corresponding graph with degrees  $(r, s) = (8, 4)$  has 39 vertices (see Figure 3), whereas the Moore bound is 42 (see Table 1). Another good example is taking the set  $S = \{0, 1, 4, 14, 16\}$ , which is a perfect difference set for  $\mathbb{Z}_{21}$ . The Moore bound for the set  $(5m, 5; 3)$  is  $24(m + 1)$  (for  $m \geq 5$ ), and it provides  $21(m + 1)$  vertices. This graph asymptotically approaches the Moore bound in  $\frac{7}{8} = 0.875$ . For  $m = 2$ , we obtain a graph with degrees  $(r, s) = (10, 5)$  having 63 vertices, whereas the maximum order is 66.

It is conjectured that perfect difference sets only exist whenever  $s - 1$  is a prime power. The conjecture has been proved true for  $s - 1 \leq 1600$  (see Evans and Mann

$s$	$\Gamma$	$S$	order of $G_m(S)$	Moore Bound (8)
3	$\mathbb{Z}_7$	$\{0, 1, 3\}$	$7(m+1)$	$7(m+1)$
4	$\mathbb{Z}_{13}$	$\{0, 1, 3, 9\}$	$13(m+1)$	$14(m+1)$
5	$\mathbb{Z}_{21}$	$\{0, 1, 4, 14, 16\}$	$21(m+1)$	$23(m+1)$
6	$\mathbb{Z}_{31}$	$\{0, 1, 6, 18, 22, 29\}$	$31(m+1)$	$34(m+1)$
8	$\mathbb{Z}_{57}$	$\{0, 1, 5, 7, 17, 35, 38, 49\}$	$57(m+1)$	$62(m+1)$
9	$\mathbb{Z}_{73}$	$\{0, 1, 17, 39, 41, 44, 48, 54, 62\}$	$73(m+1)$	$79(m+1)$
10	$\mathbb{Z}_{91}$	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$	$91(m+1)$	$98(m+1)$
12	$\mathbb{Z}_{133}$	$\{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109\}$	$133(m+1)$	$142(m+1)$

Table 3: Perfect difference sets (Singer [9]) for some values of  $s = |S|$  and the parameters of the corresponding bipartite graphs of Corollary 2.3, with degrees  $(ms, s)$ , diameter 3, and the Moore bounds (8) (for  $s - 1 \leq m \leq s^2 - s - 3$ ).

[5]), but an answer to the general question remains an open problem. In all those cases in which perfect difference sets do not exist, it would be useful to get other difference sets that are ‘close’ to being perfect, in the sense that every element of the group appears as a difference of two elements of  $S$ , but maybe this representation is not unique. There is an approximation to difference sets in the literature that fits in this way. An  $(n, s, \lambda, t)$ -almost difference set (ADS) is a subset  $S$  of size  $s$  taken from an order- $n$  group such that the multiset of differences contains  $t$  of the nonidentity group elements  $\lambda$  times and all other nonidentity group elements  $\lambda + 1$  times. The problems of existence and construction for ADS’s in arbitrary groups are even less well understood than for general difference sets. The significantly weaker difference property required, along with the relatively recent development of the ADS concept, implies that the theory of ADS’s is still a work in progress.

Inspired by the above results, we end this section by posing the following (ambitious) conjecture.

**Conjecture 1.** *For  $s - 1$  a prime power, the graphs  $G_m(S)$  of Corollary 2.3 are  $(ms, s; 3)$ -biMoore graphs*

As mentioned, the conjecture holds when  $m = 1$ , where  $G_1(S)$  is the point-line incidence graph of  $PG(2, s - 1)$ .

### 3 Covering difference sets for $s=7$

There are many values of  $s$  in which perfect difference sets  $S$  do not exist. The first one is  $s = 7$ , and it is interesting on its own. The order  $n$  for an Abelian group  $\Gamma$  having a covering difference set of order  $s = 7$  is  $n \leq 43$ . Such a covering difference set for  $n = 43$  ( $\Gamma = \mathbb{Z}_{43}$ ) would produce a perfect difference set, but we already know that it does not exist (see Evans and Mann [5]). So, we should look for covering sets of size 7 in Abelian groups of order  $n \leq 42$ . We have done an exhaustive computer search for finding a cover difference set in  $\Gamma = \mathbb{Z}_{42}$ , but we found none. To this end, notice that there are  $\binom{42}{7} \approx 27$  million candidates to test, but two properties reduce the computational cost of the exhaustive search. The first property is that  $S = \{t_1, t_2, \dots, t_s\}$  is a covering difference set if and only if  $S - t_1 = \{0, t_2 - t_1, \dots, t_s - t_1\}$  is a covering difference set. In our case, the proof is trivial from the definition and reduces the number of testing sets to  $\binom{41}{6} \approx 4.5$  million. The second property is the following result.

**Proposition 3.1.** *Let  $\Gamma$  be a group of order  $n$  with a covering set  $S$  of order  $s$ , such as  $n = s^2 - s$ . Then, every  $g \in \Gamma \setminus \{0\}$  appears once in  $D_S$  except for just one element of order 2 that appears twice.*

*Proof.* Notice that  $D_S$  has  $s^2 - s$  elements out of the main diagonal and, hence, each  $g \in \Gamma \setminus \{0\}$  must appear once in  $D_S$  except one element  $g'$  appearing twice (to fit the  $s^2 - s - 1$  different elements of  $\Gamma \setminus \{0\}$  out of the diagonal of  $D_S$ ). Moreover, since  $g' = t_i - t_j = t'_i - t'_j$  for different  $t_i, t_j, t'_i, t'_j \in S$ , then  $g'$  must have order 2 since otherwise its inverse (opposite)  $-g' = t_j - t_i = t'_j - t'_i$  would appear also twice in  $D_S$ .  $\square$

This property allows us to exclude many sets very quickly, namely, all the elements different from 21 that appear more than once during the computational building of  $D_S$ . Then, the set is automatically excluded. That is, we do not need to complete the calculation of  $D_S$  to exclude many candidate sets. Of course, Proposition 3.1 can be extended to other values of  $n$  that are ‘close’ to the maximum  $s^2 - s + 1$  by allowing a maximum number of repetitions for an element to be in  $D_S$  when checking if  $S$  can be a covering set of  $\Gamma$ . This has been very useful in performing an exhaustive search of covering sets for every Abelian group of orders 42, 41, and 40. In every case, we found none. In the first case,  $n \leq 42$ , a covering set exists when  $n = 39$ .

**Proposition 3.2.** *The maximum order  $n$  for an Abelian group  $\Gamma$  having a covering set  $S$  of order  $s = 7$  is  $n = 39$ . The set  $S = \{0, 1, 2, 4, 13, 18, 33\}$  in  $\mathbb{Z}_{39}$  provides a  $(39, 7, 1, 34)$  almost difference set (ADS).*

The set  $S = \{0, 1, 2, 4, 13, 18, 33\}$  in  $\mathbb{Z}_{39}$  provides the following difference matrix  $\mathbf{D}_S = (d_{ij})$ , where  $d_{ij} = t_i - t_j \pmod{39}$ , for  $t_i, t_j \in S$ :

$$\mathbf{D}_S = \begin{pmatrix} 0 & 38 & 37 & 35 & 26 & 21 & 6 \\ 1 & 0 & 38 & 36 & 27 & 22 & 7 \\ 2 & 1 & 0 & 37 & 28 & 23 & 8 \\ 4 & 3 & 2 & 0 & 30 & 25 & 10 \\ 13 & 12 & 11 & 9 & 0 & 34 & 19 \\ 18 & 17 & 16 & 14 & 5 & 0 & 24 \\ 33 & 32 & 31 & 29 & 20 & 15 & 0 \end{pmatrix},$$

where every non-zero element appears just once except for 1, 2, 37, 38, which appears twice. Hence, this set  $S$  is a  $(39, 7, 1, 34)$  ADS. Then, the corresponding graphs  $G_m(S)$ , with degrees  $(7m, 7)$  and diameter 3, have  $39(m + 1)$  vertices (while the Moore bound is  $48(m + 1)$ ).

Nevertheless, a bit more can be done using non-Abelian groups, as shown in the next subsection.

### 3.1 Bipartite biregular graphs derived from difference sets of non-Abelian groups

From the first contributions to the study of difference sets in  $\mathbb{Z}_m$  almost one century ago, many published papers have been devoted to difference sets in Abelian groups. Curiously enough, the situation for non-Abelian groups is quite different, where only a few contributions can be found, many of them from the 90's decade of the past century.

Although all the previous definitions related to difference sets are valid for non-Abelian groups, Proposition 2.2 cannot be applied to non-Abelian groups. The main reason is the adjacencies in (10), where the Abelian property is necessary to prove that there is a path of length two between two distinct vertices in  $V_0$ . One way to guarantee the existence of such a path is to impose the extra condition that the set of inverses of  $S$ ,  $\bar{S} = \{t_1^{-1}, t_2^{-1}, \dots, t_s^{-1}\}$ , is also a covering set. This is indeed true for Abelian groups, where if  $g \in \Gamma$  can be represented as a difference of two elements of  $S$ , that is, if  $g = t_i \cdot t_j^{-1}$ , then  $g = t_j^{-1} \cdot (t_i^{-1})^{-1}$  due to the Abelian property. Hence,  $\bar{S}$  is also a covering set.

**Corollary 3.3.** *Let  $\Gamma$  be a non-Abelian group. Then,  $G_m(S)$  is a bipartite graph with  $(m + 1)n$  vertices, where every vertex in  $V_0$  has degree  $s$  and every vertex in  $V_1$*

has degree  $ms$ . Moreover, the diameter of  $G_m(S)$  is 3 if both  $S$  and  $\bar{S}$  are covering sets of  $\Gamma$ .

*Proof.* Follow the arguments of the proof of Proposition 2.2 and note that, due to the adjacencies in (10), we can write  $(0, v \cdot t_i^{-1} \cdot t_j) = (0, v \cdot t_i^{-1} \cdot (t_j^{-1})^{-1})$ . Since  $\bar{S}$  is a covering set, a path of length 2 exists between every pair of different vertices of  $V_0$ .  $\square$

Using an exhaustive computer search, we have proved that there is no covering set  $S$  of size  $s = 7$  for the five non-Abelian groups of order 42. The largest order for a non-Abelian group with a covering set is 40, and although there are 11 groups of that order, only one has covering sets of 7. This group is a semidirect product of  $\mathbb{Z}_5$  and  $\mathbb{Z}_8$  via a square map. It has the following representation as a quotient of a free group:

$$\Gamma_1 = \langle a, b \mid a^5 = b^8 = 1, bab^{-1} = a^2 \rangle.$$

**Proposition 3.4.** *The maximum order  $n$  for a non-Abelian group having a covering set  $S$  of order  $s = 7$  is  $n = 40$ . The set  $S = \{1, b, b^4, ba, ba^{-1}b^2, ab^{-1}, bab^2\}$  in  $\Gamma_1$  is a  $(40, 7, 1, 36)$  almost difference set (ADS).*

The difference matrix

$$D_s = \begin{pmatrix} 1 & b^{-1} & b^{-4} & a^{-1}b^{-1} & b^{-2}ab^{-1} & ba^{-1} & b^{-2}a^{-1}b^{-1} \\ b & 1 & b^{-3} & ba^{-1}b^{-1} & b^{-1}ab^{-1} & b^2a^{-1} & b^{-1}a^{-1}b^{-1} \\ b^4 & b^3 & 1 & b^4a^{-1}b^{-1} & b^2ab^{-1} & b^5a^{-1} & b^2a^{-1}b^{-1} \\ ba & bab^{-1} & bab^{-4} & 1 & bab^{-2}ab^{-1} & baba^{-1} & bab^{-2}a^{-1}b^{-1} \\ ba^{-1}b^2 & ba^{-1}b & ba^{-1}b^{-2} & ba^{-1}b^2a^{-1}b^{-1} & 1 & ba^{-1}b^3a^{-1} & ba^{-2}b^{-1} \\ ab^{-1} & ab^{-2} & ab^{-5} & ab^{-1}a^{-1}b^{-1} & ab^{-3}ab^{-1} & 1 & ab^{-3}a^{-1}b^{-1} \\ bab^2 & bab & bab^{-2} & bab^2a^{-1}b^{-1} & ba^2b^{-1} & bab^3a^{-1} & 1 \end{pmatrix}$$

provides every element of  $\Gamma_1 \setminus \{1\}$  just once, except for  $b^{-1}ab^{-1}$ ,  $b^4$  and  $ba^{-1}b$  that appear twice. Note that  $b^4$  has order 2, so  $b^4 = b^{-4}$ , and  $b^{-1}ab^{-1}$  is the inverse of  $ba^{-1}b$ . Moreover, it can be check that  $\bar{S} = \{1, b^{-1}, b^4, a^{-1}b^{-1}, b^{-2}ab^{-1}, ba^{-1}, b^{-2}a^{-1}b^{-1}\}$  is also a covering set. According to Corollary 3.3, the corresponding graphs  $G_m(S)$ , with degrees  $(7m, 7)$  and diameter 3, have  $40(m + 1)$  vertices, improving the bound obtained with the Abelian group  $\mathbb{Z}_{39}$ .

## Conflict of Interest Statement

The authors have no conflict of interest.

## References

- [1] G. Araujo-Pardo, C. Dalfó, M. A. Fiol, and N. López, Bipartite biregular Moore graphs, *Discrete Math.* **344** (2021) 112582.
- [2] W. G. Brown, On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.* **9** (1966), no. 5, 281–285.
- [3] H. S. M. Coxeter, *The Real Projective Plane*, 3rd edition, Springer-Verlag, New York, 1993.
- [4] G. Erskine, P. Fratrič, and J. Širáň, Graphs derived from perfect difference sets, *Australas. J. Combin.* **80** (2021), no. 1, 48–56.
- [5] T. A. Evans and H. B. Mann, On simple difference sets, *Indian J. Stat.* **11(3/4)** (1951) 357–364.
- [6] S. Filipovski, A. Ramos Rivera, and R. Jajcay, On biregular bipartite graphs of small excess, *Discrete Math.* **342** (2019) 2066–2076.
- [7] H. Halberstam and R. Laxton, On perfect difference sets, *Quart. J. Math.* **14** (1963), no. 1, 86–90.
- [8] M. Miller and J. Širáň, Moore graphs and beyond: A survey, *Electronic J. Combin.* **20 (2)** (2013) #DS14v21.
- [9] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), no. 3, 377–385.
- [10] J. L. A. Yebra, M. A. Fiol, and J. Fàbrega, Semiregular bipartite Moore graphs, *Ars Combin.* **16A** (1983) 131–139.