Abelian Cayley digraphs with asymptotically large order for any given degree *

F. Aguiló[a], M.A. Fiol[b] and S. Pérez[c]

[a,b,c]Departament de Matemàtiques
Universitat Politècnica de Catalunya
[b]Barcelona Graduate School of Mathematics
Barcelona, Catalonia

{francesc.aguilo,miguel.angel.fiol,sonia.perez-mansilla}@upc.edu

Abstract

Abelian Cayley digraphs can be constructed by using a generalization to $\mathbb{Z}^n$ of the concept of congruence in $\mathbb{Z}$. Here we use this approach to present a family of such digraphs, which, for every fixed value of the degree, have asymptotically large number of vertices as the diameter increases. Up to now, the best known large dense results were all non-constructive.

Keywords: Cayley digraph; degree/diameter problem; density; Smith normal form; congruences in $\mathbb{Z}^n$.

1 Introduction

The degree-diameter problem for graphs (directed or undirected) has been widely studied in the last decades because of its relevance to the design of interconnection or communication networks for parallel processors. In this context one would like to have a large number of processors without requiring a large number of links, and without incurring long delays in communication from one processor to another.

The degree-diameter problem for directed graphs consists of maximizing the number of vertices of a digraph with degree at most d and diameter at most k. We refer to the survey of Miller and Sirán [15] for the current state of the art, and to the the survey of Bermond, Comellas, and Hsu [4] for details about the history of the problem.

A desirable additional property of such dense digraphs is vertex-transitivity (in particular regularity, with in-degree and out-degree of every vertex equal to d). In this case, the network is seen identically from any processor making it easy to implement all protocols, being basically the same for each node. In fact, most of the literature so far has focused on a very important class of vertex-transitive digraphs, the Cayley digraphs (see e.g. [11, 19]). Recall that a *Cayley digraph* of a group Γ with respect to a generating set A, denoted by $G = \text{Cay}(\Gamma; A)$, is the digraph whose vertices are labeled with the elements of Γ, and for which there is an arc (u, v) if and only if $v - u \in A$.

In this paper we deal exclusively with the degree-diameter problem for Cayley digraphs for which the group Γ is Abelian.

Let $NA_{d,k}$ (respectively, $NC_{d,k}$) be the maximum number of vertices that a Cayley digraph of an Abelian group (respectively, of a cyclic group), with degree d and diameter k, can have. In this framework, Wong and Coppersmith [19] proved that, for fixed degree d and large diameter k,

$$\left(\frac{k}{d}\right)^d + O(k^{d-1}) \leqslant NC_{d,k} \leqslant \frac{k^d}{d!} + O(k^{d-1}). \tag{1}$$

The exact value of $NC_{d,k}$ is only known for the case of degree $d = 2$, where the authors of [11, 16] proved that, for any $k \geqslant 2$,

$$NC_{2,k} = \left\lceil \frac{(k+2)^2}{3} \right\rceil - 1. \tag{2}$$

The *density*, $\delta(G)$, of a Cayley digraph G on a d-generated finite Abelian group of order N and diameter $k(G)$ is defined by

$$\delta(G) = \frac{N}{(k(G) + d)^d}. \tag{3}$$

For $d = 2$, from (2) and (3), we have $\delta \leqslant \frac{1}{3}$. For $d = 3$, Fiduccia, Forcade and Zito [12, Corollary 3.6] gave the upper bound $NA_{3,k} \leqslant \frac{3}{25}(k+3)^3$ and so, for this degree, it follows that $\delta \leqslant \frac{3}{25} = 0.12$. Several authors have given various families of Cayley digraphs of cyclic groups with small diameter for fixed degree d and order N. Cayley digraphs of cyclic groups can also be found in the literature under the name of *loop networks*. Table 1 summarizes some of the results for the well-studied case $d = 3$. The entry of δ^* indicates that the result represents the asymptotical value for the density of these constructions for large values of k.

Notice that the fact $N = \alpha k^d + O(k^{d-1})$ does not necessarily imply $\delta = \alpha$. For instance, a result of Dougherty and Faber [6, Corollary 8.2] gives the existence of cyclic Cayley digraphs of degree $d = 3$ and order $N = 0.084k^3 + O(k^2)$ for all k. Table 2 gives numerical evidence that this result is not difficult to achieve; however, equality $\delta = 0.084$ is apparently not so easy to attain. As far as we know, for the cyclic case, there is only one known value of $4 \leqslant N \leqslant 8000$ that achieves this density, that is $N = 84$ with $G = \text{Cay}(\mathbb{Z}_{84}, \{2, 9, 25\})$ and $k(G) = 7$. Moreover, no known order achieves the upper

Authors	δ^*	Conditions on k
Gómez, Gutiérrez & Ibeas [13]	0.0370	$k \equiv 0, 1, 2 \pmod 3$
Aguiló, Fiol & García [2]	0.0740	$k \equiv 2, 4, 5 \pmod 6$
Chen & Gu [5]	0.0780	No condition on k
Aguiló [1]	0.0807	$k = 22t + 12,\ t \not\equiv 2, 7 \pmod{10}$
Aguiló, Simó & Zaragozá [3]	0.0840	$k \equiv 2 \pmod{30}$

Table 1: Several explicit cyclic constructions for $d = 3$

k	δ	$\lceil 0.084k^3 \rceil$	$\lceil \frac{3}{25}k^3 \rceil$	$\lfloor \frac{3}{25}(k+3)^3 \rfloor$	$NC_{3,k}$
1	0.06250	1	1	7	4
2	0.07200	1	1	13	9
3	0.07407	3	4	24	16
4	0.07872	6	8	38	27
5	0.07812	11	15	56	40
6	0.07819	19	26	81	57
7	0.08400	29	42	111	84
8	0.08340	44	62	147	111
9	0.07986	62	88	192	138
10	0.08011	84	120	244	176

Table 2: Several density values for $d = 3$ and $1 \leqslant k \leqslant 10$ in the cyclic case

bound of Fiduccia, Forcade and Zito for the cyclic case. As far as we know, no explicit construction is known achieving $\delta^* = 0.084$, in the sense of Table 1, for all k.

It is worth to mention the work of Rödseth [18] on weighted loop networks, where he gave sharp lower bounds for the diameter and mean distance for $d = 2$ and general bounds for $d \geqslant 3$ as well.

As mentioned above, the concern of our paper is Cayley digraphs of Abelian groups. In fact, the bounds in (1) also apply for $NA_{d,k}$. In [14, Theorem 1.1] Mask, Schneider, and Jia claimed to show that, for any d and k, $NA_{d,k} = NC_{d,k}$, but Fiol in [10] corrected this claim by giving some counterexamples for the case $d = 2$. In fact, Fiol et al., in [11, 16], show (see also the comments of Dougherty and Faber in [6]):

Proposition 1. *For any diameter $k \geqslant 2$,*

$$NA_{2,k} = \begin{cases} NC_{2,k} + 1, & \text{if } k \equiv 1 \pmod 3, \\ NC_{2,k}, & \text{otherwise.} \end{cases} \tag{4}$$

In general, if Γ is an Abelian group and $|A| = d$, the Cayley digraph $\mathrm{Cay}(\Gamma, A)$ has order (count the number of vertices at distances 0 to k and add them up [11]):

$$NA_{d,k} < \binom{k+d}{d} = \binom{k+d}{k}.$$

Then, it is not difficult to see that:

$$k > \sqrt[d]{d! NA_{d,k}} - \frac{1}{2}(d+1).$$

Nevertheless, as far as we know, the best upper bound known for the order of Cayley digraphs of Abelian groups is the one of Dougherty and Faber in [6, Theorem 21], where they proved the following non-constructive result:

There is a positive constant c (not depending on d or k), such that, for any fixed $d \geqslant 2$ and any k, there exist Cayley digraphs of Abelian groups on d generators having diameter at most k and number of vertices $NA_{d,k}$ satisfying

$$NA_{d,k} \geqslant \frac{c}{d(\ln d)^{1+\log_2 e}} \frac{k^d}{d!} + O(k^{d-1}).$$

In our study, we use the following approach developed by Aguiló, Esqué and Fiol [7, 8]: Every Cayley digraph G from an Abelian group Γ is fully characterized by an integral $n \times n$ matrix $\boldsymbol{M}$ such that $\Gamma = \mathbb{Z}^n / \boldsymbol{M}\mathbb{Z}^n$ (the so-called 'group of integral n-vectors modulo $\boldsymbol{M}$' that is detailed in Section 2). This representation makes it clear that the digraph G is isomorphic to $\mathrm{Cay}(\mathbb{Z}^n / \boldsymbol{M}\mathbb{Z}^n, A)$, where A is the set of unitary coordinate vectors $\boldsymbol{e}_i$, $i = 1, \ldots, n$.

The plan of the paper is as follows. In the following section, and for the sake of completeness, we will recall the algebraic background on which the above isomorphism is based. Afterwards, in contrast with the theoretical bound of Dougherty and Faber, we will present an explicit infinite family of Cayley digraphs of Abelian groups whose order is asymptotically large. This family will be constructed by using a generalization to $\mathbb{Z}^n$ of the concept of congruence in $\mathbb{Z}$.

2 Some theoretical background

In this section we recall some basic concepts and results on which our study is based (see [7, 8, 9] for further details).

2.1 Congruences in $\mathbb{Z}^n$

Given a nonsingular integral $n \times n$ matrix $\boldsymbol{M}$, we say that the integral vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$ are *congruent modulo $\boldsymbol{M}$* (see [9]) when their difference belongs to the lattice generated by $\boldsymbol{M}$, that is,

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{M}} \quad \Longleftrightarrow \quad \boldsymbol{a} - \boldsymbol{b} \in \boldsymbol{M}\mathbb{Z}^n. \tag{5}$$

So, as the quotient group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is the cyclic group of integers modulo m, the quotient group $\mathbb{Z}_{\boldsymbol{M}}^n = \mathbb{Z}^n / \boldsymbol{M}\mathbb{Z}^n$ can intuitively be called the *group of integral vectors modulo $\boldsymbol{M}$* (where each equivalence class is identified by any of its representatives).

In particular, notice that, when $\boldsymbol{M} = \mathrm{diag}(m_1, m_2, \ldots, m_n)$, (5) implies that the vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^\top$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)^\top$ are congruent modulo $\boldsymbol{M}$ if and only if

$$a_i \equiv b_i \pmod{m_i} \qquad (1 \leqslant i \leqslant n).$$

Moreover, in this case $\mathbb{Z}_{\boldsymbol{M}}^n$ is the direct product of the cyclic groups $\mathbb{Z}_{m_i}$, $i = 1, 2, \ldots, n$.

2.2 The Smith normal form

As before, let $\boldsymbol{M} = (m_{ij})$ be a nonsingular matrix of $\mathbb{Z}^{n \times n}$, with $N = \det \boldsymbol{M}$. Let $k \in \mathbb{Z}$, $1 \leqslant k \leqslant n$. The kth *determinantal divisor* of $\boldsymbol{M}$, denoted by $d_k(\boldsymbol{M}) = d_k$, is defined as the greatest common divisor of the $\binom{n}{k}^2$ $k \times k$ determinantal minors of $\boldsymbol{M}$. Notice that $d_k \mid d_{k+1}$ for all $k = 1, 2, \ldots, n-1$ and $d_n = N$. For convenience, put $d_0 = 1$. The *invariant factors* of $\boldsymbol{M}$ are the quantities

$$s_k(\boldsymbol{M}) = s_k = \frac{d_k}{d_{k-1}}, \qquad k = 1, 2, \ldots, n.$$

It can be shown that $s_i \mid s_{i+1}$, $i = 1, 2, \ldots, n-1$.

By the *Smith normal form* theorem, $\boldsymbol{M}$ is equivalent to the diagonal matrix $\boldsymbol{S}(\boldsymbol{M}) = \boldsymbol{S} = \mathrm{diag}(s_1, s_2, \ldots, s_n)$, i.e. there are two unimodular matrices $\boldsymbol{U}, \boldsymbol{V} \in \mathbb{Z}^{n \times n}$ such that $\boldsymbol{S} = \boldsymbol{U} \boldsymbol{M} \boldsymbol{V}$. This canonical form $\boldsymbol{S}$ is unique and the unimodular matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ are not. The following proposition is a consequence of this theorem (see e.g. Newman [17])

Proposition 2. (Fiol [8]) *Set $\boldsymbol{M} \in \mathbb{Z}^{n \times n}$ with $N = |\det \boldsymbol{M}|$.*

(a) *The number of equivalence classes modulo $\boldsymbol{M}$ is $|\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n| = N$.*

(b) *If $p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ is the prime factorization of N, then $\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n \cong \mathbb{Z}^r / \boldsymbol{S}' \mathbb{Z}^r$ for some $r \times r$ matrix $\boldsymbol{S}'$ with $r \leqslant \max\{r_i : 1 \leqslant i \leqslant t\}$.*

(c) *The (Abelian) group of integral vectors modulo $\boldsymbol{M}$ is cyclic if and only if $d_{n-1} = 1$.*

(d) *Let r be the smallest integer such that $s_{n-r} = 1$. Then r is the rank of $\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n$ and the last r columns of $\boldsymbol{U}^{-1}$ form a basis of $\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n$.*

In other words, when $s_1 = \cdots = s_{n-k-1} = 1$ and $s_{n-k} > 1$, we have

$$\boldsymbol{S}' = \mathrm{diag}(s_{n-k}, \ldots, s_n)$$

and $\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n \cong \mathbb{Z}^r / \boldsymbol{S}' \mathbb{Z}^r \cong \mathbb{Z}_{s_{n-r}} \oplus \cdots \oplus \mathbb{Z}_{s_n}$. The isomorphism is given by $\phi(\boldsymbol{x}) = \boldsymbol{U} \boldsymbol{x}$ and it will be used in the next section.

3 A new family of Abelian Cayley digraphs

Given a nonsingular integral matrix $\boldsymbol{M} \in \mathbb{Z}^{n \times n}$, the Cayley digraph

$$G_{\boldsymbol{M}} = \mathrm{Cay}(\mathbb{Z}^n / \boldsymbol{M} \mathbb{Z}^n, A),$$

with $A = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ the set of unitary coordinate vectors, is known as the *digraph of commutative steps* of $\boldsymbol{M}$.

Now let us consider the circulant matrix $\boldsymbol{M} = \mathrm{circ}(n, -1, -1, \ldots, -1)$, which defines the digraph of commutative steps $G_{\boldsymbol{M}} = \mathrm{Cay}(\mathbb{Z}^n/\boldsymbol{M}\mathbb{Z}^n, \{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\})$. Clearly, $G_{\boldsymbol{M}}$ is regular with degree $d = n$. Moreover, its order is

$$N = \det \boldsymbol{M} = \det \begin{pmatrix} n & -1 & -1 & \cdots & -1 \\ -1 & n & -1 & \cdots & -1 \\ -1 & -1 & n & \cdots & -1 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & -1 & -1 & \cdots & n \end{pmatrix} = \det \begin{pmatrix} 1 & -1 & -1 & \cdots & -1 \\ 1 & n & -1 & \cdots & -1 \\ 1 & -1 & n & \cdots & -1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & -1 & -1 & \cdots & n \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & n+1 & 0 & \cdots & 0 \\ 1 & 0 & n+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \cdots & n+1 \end{pmatrix} = (n+1)^{n-1}.$$

Given $\boldsymbol{x} = (x_1, \ldots, x_n)$, let $\|\boldsymbol{x}\|_1 = \sum_{i=1}^n |x_i|$. The following result gives the diameter of $G_{\boldsymbol{M}}$.

Proposition 3. *Given the circulant matrix $\boldsymbol{M} = \mathrm{circ}(n, -1, -1, \ldots, -1)$, the digraph of commutative steps $G_{\boldsymbol{M}}$ defined as above has diameter $k = \binom{n}{2} = n(n-1)/2$.*

Proof. Let $H \subset \mathbb{Z}^n$ be a set of N nonnegative integral vectors, which are different modulo $\boldsymbol{M}$. Let $k(H) = \max\{\|\boldsymbol{x}\|_1 = \sum_i x_i : \boldsymbol{x} \in H\}$. Then, the diameter of $G_{\boldsymbol{M}}$ is $k(G_{\boldsymbol{M}}) = \min\{k(H) : H \subset \mathbb{Z}^n\}$. Let us assume that L is a set that attains such a minimum, that is, $k = k(L)$. Thus, L corresponds to an optimal set of lattice points, in the sense that the distance from the origin to a lattice point (vector) equals the distance from vertex zero to the corresponding vertex of $G_{\boldsymbol{M}}$. Then, we see that $\boldsymbol{x} \in L$ if and only if $0 \leqslant x_i \leqslant n-1$ for $i = 1, \ldots, n$, and

(1) There is at most 1 entry such that $x_i \geqslant n-1$,

(2) There are at most 2 entries such that $x_i \geqslant n-2$,

$\vdots$

$(n-1)$ There are at most $n-1$ entries such that $x_i \geqslant 1$.

Indeed, $\boldsymbol{x} \in L$ cannot have any entry, say $x_1 \geqslant n$, since, otherwise, the vector

$$\boldsymbol{y} = \boldsymbol{x} - (n, -1, -1, \ldots, -1) \equiv \boldsymbol{x} \pmod{\boldsymbol{M}}$$

would satisfy $\sum y_i = \sum x_i - 1$. Moreover,

(1) There cannot be 2 entries, say $x_1, x_2 \geqslant n-1$, since, otherwise, the vector

$$\boldsymbol{y} = \boldsymbol{x} - (n, -1, -1, \ldots, -1) - (-1, n, -1, \ldots, -1) \equiv \boldsymbol{x} \pmod{\boldsymbol{M}}$$

would satisfy $\sum y_i = \sum x_i - 2$,

(2) There cannot be 3 entries, say $x_1, x_2, x_3 \geqslant n - 2$, since, otherwise, the vector

$$\boldsymbol{y} = \boldsymbol{x} - (n, -1, \ldots, -1) - (-1, n, -1, \ldots, -1) - (-1, -1, n, \ldots, -1) \equiv \boldsymbol{x} \pmod{\boldsymbol{M}}$$

would satisfy $\sum y_i = \sum x_i - 3$,

and so on. Now we will show that, under the above conditions, the cardinality of L is $N = \det \boldsymbol{M} = (n+1)^{n-1}$. With this aim, for every pair of integers $0 \leqslant m \leqslant n$, let $f(m, n)$ be the number of integral vectors with m entries, $(x_1, \ldots, x_m) \in \mathbb{Z}^m$, $0 \leqslant x_i \leqslant n - 1$, having at most i entries $x_j \geqslant n - i$ for every $1 \leqslant i \leqslant m$. (Notice that if $m = n$, the case $i = n$ does not imply any restriction.) Such a number satisfies the following recurrences (by definition, we take $f(0, n) = 1$).

If $m < n$,

$$f(m, n) = \sum_{i=0}^{m} \binom{m}{m-i} f(i, n-1). \tag{6}$$

If $m = n$,

$$f(m, n) = \sum_{i=0}^{m-1} \binom{m}{m-i} f(i, n-1). \tag{7}$$

Now, by induction, we can prove that

$$f(m, n) = (n - m + 1)(n + 1)^{m-1}. \tag{8}$$

- $f(0, n) = 1$ (by definition).

- $f(1, n) = n$ (obvious).

- Let assume that (8) holds for $m - 1$. Then:

  If $m < n$,

  $$f(m, n) = \sum_{i=0}^{m} \binom{m}{i} f(i, n-1) = \sum_{i=0}^{m} \binom{m}{i} (n-i)n^{i-1} = \sum_{i=0}^{m} \binom{m}{i} n^i - \sum_{i=0}^{m} \binom{m}{i} i n^{i-1}$$
  $$= (n+1)^m - m(n+1)^{m-1} = (n + 1 - m)(n+1)^{m-1}.$$

  If $m = n$,

  $$f(m, n) = \sum_{i=0}^{n-1} \binom{n}{n-i} f(i, n-1) = \sum_{i=0}^{n-1} \binom{n}{n-i} (n-i)n^{i-1}$$
  $$= \sum_{i=0}^{n-1} \binom{n-1}{i} n^i = (n+1)^{n-1}.$$

Hence, we have established (8). From (8) it follows that $|L| = f(n,n) = (n+1)^{n-1} = \det \boldsymbol{M}$.

Finally, notice that, according to the characterization above, $k(L)$ equals the distance from the origin to the vectors of the form $\boldsymbol{x} = (n-1, n-2, \ldots, 0)$ (up to permutation of the entries). Then,

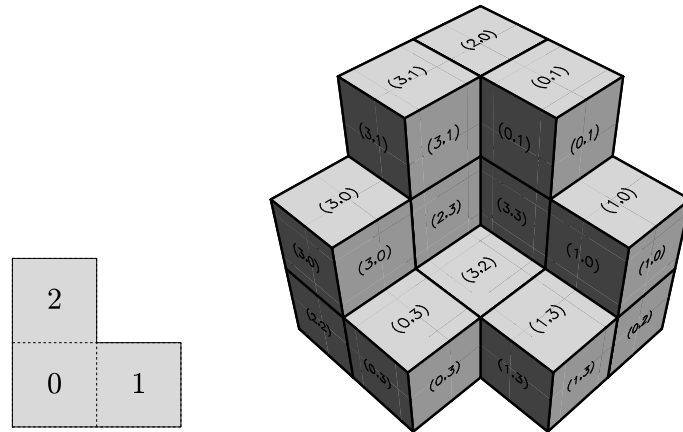$$k(G_{\boldsymbol{M}}) = k(L) = \sum_{i=1}^{n} x_i = 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2} = \binom{n}{2},$$

as claimed. □

Figure 1: Minimum distance diagrams related to D_2 and D_3

Notice that, from the above proof, the number of vertices in $G_{\boldsymbol{M}}$ at maximum distance $k = \binom{n}{2}$ from every vertex is $n!$.

From now on, let $s\mathbb{Z}_t = \mathbb{Z}_t \oplus \overset{(s)}{\cdots} \oplus \mathbb{Z}_t$.

Theorem 4. *Set* $B_n = \{(1,1,\ldots,1), (2,1,\ldots,1), \ldots, (1,\ldots,1,2)\} \subset \mathbb{Z}^{n-1}$. *Then, the Cayley digraph* $D_n = \mathrm{Cay}((n-1)\mathbb{Z}_{n+1}, B_n)$ *has diameter* $k_n = \binom{n}{2}$.

Proof. Taking the matrix $\boldsymbol{M}_n = \mathrm{circ}(n, -1, \ldots, -1) \in \mathbb{Z}^{n \times n}$, it is not difficult to see it has the Smith Normal Form $\boldsymbol{S}_n = \boldsymbol{U}_n \boldsymbol{M}_n \boldsymbol{V}_n = \mathrm{diag}(1, n+1, \ldots, n+1)$ with unimodular matrices

$$\boldsymbol{U}_n = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{pmatrix} \quad \text{and} \quad \boldsymbol{V}_n = \begin{pmatrix} 1 & -1 & -1 & \cdots & -1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}. \quad (9)$$

Thus, we have the isomorphism of digraphs $G_{\boldsymbol{M}_n} \cong D'_n = \mathrm{Cay}(\mathbb{Z}_1 \oplus (n-1)\mathbb{Z}_{n+1}, B'_n)$, with $B'_n = \{(1,1,1,\ldots,1), (1,2,1,\ldots,1), \ldots, (1,1,1,\ldots,1,2)\} \subset \mathbb{Z}^n$, given by $\phi(\boldsymbol{e}_i) = \boldsymbol{U}_n \boldsymbol{e}_i = \boldsymbol{b}_i$ ($\boldsymbol{b}_i$ are the elements of B'_n). Therefore, by Proposition 2, the diameter of D'_n is $k_n = \binom{n}{2}$. Now the statement follows from the direct digraph isomorphism $D'_n \cong D_n$. □

Figure 1 shows minimum distance diagrams related to $D_2 = \text{Cay}(\mathbb{Z}_3, \{1, 2\})$ and $D_n = \text{Cay}(\mathbb{Z}_4 \oplus \mathbb{Z}_4, \{(1, 1), (2, 1), (1, 2)\})$ with diameters $k(D_2) = 1$ and $k(D_3) = 3$.

Proposition 5. *Let us denote $\boldsymbol{M}_n = \text{circ}(n, -1, \ldots, -1)$, $n \geqslant 2$, the matrix of Proposition 2. Consider the matrix $\boldsymbol{M}_{n,m} = m\boldsymbol{M}_n = \text{circ}(mn, -m, \ldots, -m) \in \mathbb{Z}^{n \times n}$, for $m \geqslant 1$. Then, the commutative step digraph $G_{\boldsymbol{M}_{n,m}}$ has order $N_{n,m} = m^n(n+1)^{n-1}$ and diameter $k_{n,m} = \binom{n+1}{2}m - n$.*

Proof. Let us denote the columns $\boldsymbol{M}_{n,m} = (\boldsymbol{c}_1 | \cdots | \boldsymbol{c}_n)$, that is the i-th column of $\boldsymbol{M}_{n,m}$ is denoted by $\boldsymbol{c}_i = (-m, \ldots, -m, \overset{i}{\overbrace{mn}}, -m, \ldots, -m)^\top$. Let us assume that L is a hyper-L for the digraph $G_{\boldsymbol{M}_{n,m}}$, in the same sense as in the proof of Proposition 2. Set $\boldsymbol{x} = (x_1, \ldots, x_n) \in L$. Then, all the entries of $\boldsymbol{x}$ must be $x_i \leqslant mn - 1$. If say $x_1 \geqslant mn$, then $\boldsymbol{y} = \boldsymbol{x} - \boldsymbol{c}_1 = (x_1 - mn, x_2 + m, \ldots, x_n + m) \in \mathbb{Z}_{\geqslant 0}^n$. Then, $\boldsymbol{y} \equiv \boldsymbol{x} \pmod{\boldsymbol{M}_{n,m}}$ and $\|\boldsymbol{y}\|_1 = \|\boldsymbol{x}\|_1 - m$, thus $\boldsymbol{x} \notin L$; a contradiction.

There cannot be more than k entries of $\boldsymbol{x}$ with $x_i \geqslant m(n-k+1) - 1$, for $k \in \{1, \ldots, n-1\}$. Otherwise, if it were the case that for instance $x_1, \ldots, x_{k+1} \geqslant m(n - k + 1) - 1$, then the vector

$$\boldsymbol{y}_k = \boldsymbol{x} - \boldsymbol{c}_1^\top - \ldots - \boldsymbol{c}_{k+1}^\top = (x_1 - mn + km, \ldots, x_{k+1} - mn + km, x_{k+2} + km, \ldots, x_n + km)$$

would be $\boldsymbol{y}_k \equiv \boldsymbol{x} \pmod{\boldsymbol{M}_{n,m}}$, $\boldsymbol{y}_k \in \mathbb{Z}_{\geqslant 0}^n$ and $\|\boldsymbol{y}_k\|_1 = \|\boldsymbol{x}\|_1 - m[k(n - k) + 1]$. Thus $\boldsymbol{x} \notin L$, a contradiction.

Therefore, the maximum $\max\{\|\boldsymbol{x}\|_1 : \boldsymbol{x} \in L\}$ is attained at vectors of type $\boldsymbol{x}^* = (mn - 1, m(n-1) - 1, \ldots, m2 - 1, m - 1)$ (up to permutations of the entries). So, the diameter is

$$k_{n,m} = k(L) = \|\boldsymbol{x}^*\|_1 = \binom{n+1}{2}m - n = n\left(\frac{n+1}{2}m - 1\right).$$

Using similar arguments as in the proof of Proposition 2, it can be seen that there are $N_{n,m} = \det \boldsymbol{M}_{n,m} = m^n(n+1)^{n-1}$ different vectors in L, the order of the commutative step digraph $G_{\boldsymbol{M}_{n,m}}$. $\qquad\square$

Theorem 6. *Consider the generator set $B_n' \subset \mathbb{Z}^n$ given in the proof of Theorem 4. Then, the Cayley digraph $D_{n,m} = \text{Cay}(\mathbb{Z}_m \oplus (n-1)\mathbb{Z}_{m(n+1)}, B_n')$ has diameter $k_{n,m} = \binom{n+1}{2}m - n$.*

Proof. Using the same argument in the proof of Theorem 4, the statement follows from the Smith normal form of the matrix $\boldsymbol{M}_{n,m}$, i.e. $\boldsymbol{S}_{n,m} = \text{diag}(m, m(n+1), \ldots, m(n+1)) = \boldsymbol{U}_n \boldsymbol{M}_{n,m} \boldsymbol{V}_n$. The unimodular matrices $\boldsymbol{U}_n$ and $\boldsymbol{V}_n$ are as in (9). The digraph isomorphism is now $D_{n,m} \cong G_{\boldsymbol{M}_{n,m}}$, where $G_{\boldsymbol{M}_{n,m}}$ is the commutative step digraph of Proposition 5. $\qquad\square$

In terms of the degree $d = n$ and diameter k, we get the number of vertices and density of $D_{n,m}$:

$$N_{d,k} = \frac{2^d}{d+1}\left(\frac{k}{d} + 1\right)^d \quad \text{and} \quad \delta_d = \frac{1}{d+1}\left(\frac{2}{d}\right)^d \text{ for all } k. \tag{10}$$

Note that, given a fixed degree d, the value of the density remains constant as the diameter k increases.

As mentioned before in the Introduction, Dougherty and Faber gave the following nonconstructive result in [6]: There is a positive constant c (not depending on d or k), such that, for any fixed $d \geqslant 2$ and any k, there exist Cayley digraphs of Abelian groups having diameter at most k and number of vertices satisfying:

$$N_{d,k} \geqslant \frac{c}{d(\ln d)^{1+\log_2 e}} \frac{k^d}{d!} + O(k^{d-1}).$$

which, using Stirling's formula, gives

$$N_{d,k} \geqslant \frac{c}{\sqrt{2\pi}} e^{d - \frac{3}{2}\ln d - (\ln\ln d)(1+\log_2 e)} \left(\frac{k}{d}\right)^d + O(k^{d-1}), \tag{11}$$

with multiplicative factor of $\left(\frac{k}{d}\right)^d$ being

$$\frac{c}{\sqrt{2\pi}} e^{d - \frac{3}{2}\ln d - (\ln\ln d)(1+\log_2 e)} \sim e^{d - \frac{3}{2}\ln d}.$$

For large k, the order in (10) is

$$N_{d,k} = 2^{d - \log_2(d+1)} \left(\frac{k}{d}\right)^d + O(k^{d-1}), \tag{12}$$

where the multiplicative factor of $\left(\frac{k}{d}\right)^d$ is

$$2^{d - \log_2(d+1)} \sim 2^{d - \frac{1}{\ln 2}\ln d}.$$

Although this last coefficient turns out to be smaller than the one appearing in the theoretical bound of Dougherty and Faber, the explicit constructions given here achieve it, and they are asymptotically the only ones known up to date.

References

[1] F. Aguiló-Gost. New dense families of triple loop networks. *Discrete Math.*, **197/198**:15–27, 1999.

[2] F. Aguiló, M.A. Fiol, and C. García. Triple loop networks with small transmission delay. *Discrete Math.* **167/168**:3–16, 1997.

[3] F. Aguiló, E. Simó, and M. Zaragozá. On Dense Triple-Loop Networks. *Electronic Notes in Discrete Math.* **10**:261–264, 2001.

[4] J.-C. Bermond, F. Comellas, and D.F. Hsu. Distributed loop computer networks: a survey. *J. Parallel Distribut. Comput.* **24**:2–10, 1995.

[5] S. Chen and W. Gu. Exact order of subsets of asymptotic bases. *J. Number Theory* **41**:15–21, 1992.

[6] R. Dougherty and V. Faber. The degree-diameter problem for several varietes of Cayley graphs I: The Abelian case. *SIAM J. Discrete Math.* **17**(3):478–519, 2004.

[7] P. Esqué, F. Aguiló, and M.A. Fiol. Double commutative-step digraphs with minimum diameters. *Discrete Math.* **114**:147–157, 1993.

[8] M.A. Fiol. On congruences in $\mathbb{Z}^n$ and the dimension of a multidimensional circulant. *Discrete Math.* **141**:123–134, 1995.

[9] M.A. Fiol. Congruences in $\mathbb{Z}^n$, finite Abelian groups and the Chinese remainder theorem. *Discrete Math.* **67**:101–105, 1987.

[10] M.A. Fiol. Comments on "Extremal Cayley digraphs of finite Abelian groups" [Intercon. Networks 12 (2011), no. 1-2, 125–135]. *J. Intercon. Networks* **14**(4):1350016, 2013.

[11] M.A. Fiol, J.L.A. Yebra, I. Alegre and M. Valero. A discrete optimization problem in local networks and data alignment. *IEEE Trans. Comput.* **C-36**:702–713, 1987.

[12] C.M. Fiduccia, R.W. Forcade, and J.S. Zito. Geometry and diameter bounds of directed Cayley graphs of Abelian groups. *SIAM J. Discrete Math.* **11**:157–167, 1988.

[13] D. Gómez, J. Gutiérrez and Á. Ibeas. Cayley of finite Abelian groups and monomial ideals. *SIAM J. Discrete Math.* **21**(3):763–784, 2007.

[14] A.G. Mask, J. Schneider and X. Jia. Extremal Cayley digraphs of finite Abelian groups. *J. Intercon. Networks* **12**(1-2):125–135, 2011.

[15] M. Miller and J. Sirán. Moore graphs and beyond: A survey of the degree/diameter problem. *Electron. J. Combin.* **20**(2):#DS14v2, 2013.

[16] P. Morillo, M.A. Fiol and J. Fàbrega. The diameter of directed graphs associated to plane tesselations. *Ars Combin.* **20A**(4):17–27, 1985.

[17] M. Newman. *Integral Matrices.* Pure and Appl. Math. Series Vol. **45**, Ac. Press (1972), New York.

[18] Ö. J. Rödseth. Weighted multi-connected loop networks. *Discrete Math.* **148**:161–173, 1996.

[19] C. K. Wong and D. Coppersmith. A combinatorial problem related to multimodule memory organitzations. *J. Assoc. Comput. Machin.* **21**:392–402, 1974.