

# Frobenius circulant graphs of valency four

Alison Thomson and Sanming Zhou

Department of Mathematics and Statistics  
The University of Melbourne  
Parkville, VIC 3010, Australia  
{a.thomson, smzhou}@ms.unimelb.edu.au

*Dedicated to Cheryl E. Praeger with love and best wishes on the occasion of her 60th birthday.*

## Abstract

A first kind Frobenius graph is a Cayley graph  $\text{Cay}(K, S)$  on the Frobenius kernel of a Frobenius group  $K \rtimes H$  such that  $S = a^H$  for some  $a \in K$  with  $\langle a^H \rangle = K$ , where  $H$  is of even order or  $a$  is an involution. It is known that such graphs admit ‘perfect’ routing and gossiping schemes. A circulant graph is a Cayley graph on a cyclic group of order at least three. Since circulant graphs are widely used as models for interconnection networks, it is thus highly desirable to characterize those of them which are Frobenius of the first kind. In this paper we first give such a characterization for connected 4-valent circulant graphs, and then describe optimal routing and gossiping schemes for those of them which are first kind Frobenius graphs. Examples of such graphs include the 4-valent circulant graph with a given diameter and maximum possible order.

**Key words:** Cayley graph; circulant graph; multi-loop network; double-loop network; Frobenius group; Frobenius graph; complete rotation; gossiping; minimum gossip time; routing; edge-forwarding index; arc-forwarding index

**AMS Subject Classification (2000):** 05C25, 68M10, 90B18

## 1 Introduction

There is a long history in searching for ‘good’ graphs to model interconnection networks. It is widely believed [1, 2, 9] that Cayley graphs, in particular circulant graphs [8, 22], are good candidates. (A *Cayley graph* on a group  $K$  is a graph  $\text{Cay}(K, S)$  with vertex set  $K$  such that  $x, y \in K$  are adjacent if and only if  $xy^{-1} \in S$ , where the *connection set*  $S \subseteq K \setminus \{1\}$  is closed under taking inverse. A *circulant graph* is a Cayley graph on a cyclic group of order at least three.) In [19], Solé proved that for a certain class of graphs, called orbital-regular graphs, there exists an all-to-all shortest path routing such that the load on all edges is uniform and hence the edge-forward index [11] achieves the minimum. Here an *all-to-all routing* (or a routing for short) of a graph  $\Gamma$  is a set of oriented paths such that there is exactly one path between each ordered pair of vertices; the *load of an edge* is the number of times it is traversed by such paths in either direction; the *load of a routing* is the maximum load on an edge; and the *edge-forward index*  $\pi(\Gamma)$  is [11] the minimum load over all possible all-to-all routings of  $\Gamma$ . The *arc-forwarding index*  $\vec{\pi}$  is defined similarly by taking into account the direction when counting the number of times an arc is traversed, where an *arc* is an ordered pair of adjacent vertices. A routing is called a

*shortest path routing* if all paths in it are shortest paths. The *minimal edge-* and *arc-forwarding indices* [9],  $\pi_m$ ,  $\vec{\pi}_m$ , are defined by restricting to shortest path routings in the definitions of  $\pi$  and  $\vec{\pi}$  respectively. A routing under which all edges have the same load is called *edge-uniform*. *Arc-uniform* routings are understood similarly.

In [7], Fang, Li and Praeger proved that a graph is orbital-regular if and only if it is a cycle, a star, or a Frobenius graph. A group  $G$  acting transitively but not regularly on a set  $V$  such that only the identity element of  $G$  can fix two points of  $V$  is called [6, 18] a *Frobenius group*. It is well-known [6, Section 3.4] that a finite Frobenius group  $G$  has a nilpotent normal subgroup  $K$ , called the *Frobenius kernel* of  $G$ , which is regular on  $V$ . Hence  $G = K \rtimes H$  (semidirect product of  $K$  by  $H$ ), where  $H$  is the stabiliser of a point of  $V$  and is called a *Frobenius complement* for  $K$  in  $G$ . Since  $K$  is regular on  $V$ , we may identify  $V$  with  $K$  in such a way that  $K$  acts on itself by right multiplication, and we choose  $H$  to be the stabiliser of 1 (identity element of  $K$ ) so that  $H$  acts on  $K$  by conjugation. A *G-Frobenius graph* [7] is a Cayley graph  $\Gamma = \text{Cay}(K, S)$  on  $K$ , where

$$S = \begin{cases} a^H, & \text{if } |H| \text{ is even or } |a| = 2 \\ a^H \cup (a^{-1})^H, & \text{if } |H| \text{ is odd and } |a| \neq 2 \end{cases}$$

for some  $a \in K$  satisfying  $\langle a^H \rangle = K$ , where  $x^H = \{h^{-1}xh : h \in H\}$  for  $x \in K$  and  $|a|$  is the order of  $a$ . We call  $\Gamma$  a *first* or *second kind* [25] Frobenius graph, respectively, if  $S$  is as in the first or second line above. Since  $\langle a^H \rangle = K$ ,  $\Gamma$  is always connected. As examples, Paley graphs are Frobenius [19], and those Hamming graphs  $H(d, q)$  which are Frobenius are classified in [14], where  $q$  is a prime power. It is known that  $\pi(\Gamma) = \sum_{u,v \in K} d(u, v) / |E(\Gamma)| = 2 \sum_{i=1}^d in_i$  or  $\sum_{i=1}^d in_i$  [7], depending on whether  $\Gamma$  is of the first or second kind, where  $d(u, v)$  is the distance in  $\Gamma$  between  $u$  and  $v$ ,  $d$  is the diameter of  $\Gamma$ , and  $n_i$  is the number of  $H$ -orbits contained in the set of vertices at distance  $i$  from 1.  $(n_1, n_2, \dots, n_d)$  is called [7] the *type* of  $\Gamma$ .

Besides the forwarding indices above, another important measure of performance of a network is its behavior with respect to gossiping. Here by gossiping we mean an information dissemination process for which each vertex has a distinct message to be sent to all other vertices. In this paper we consider the *store-and-forward, all-port and full-duplex* model [3]: a vertex must receive a message wholly before retransmitting it to other vertices; a vertex can exchange messages (which may be different) with all of its neighbours at each time step; messages can traverse an edge in both directions simultaneously; no two messages can transmit over the same arc at the same time; and it takes one time step to transmit any message over an arc. A *gossiping scheme* is a procedure fulfilling the gossiping under these constraints, and the *minimum gossip time* [3] of a graph  $\Gamma$ ,  $t(\Gamma)$ , is the minimum number of time steps required by such a scheme.

In [25] the second-named author devised optimal routing and gossiping schemes with attractive features for any first kind Frobenius graph. The results in [25] suggest that not only does such a graph has smallest possible forwarding indices  $\pi$ ,  $\vec{\pi}$ ,  $\pi_m$  and  $\vec{\pi}_m$ , but also it attains the minimum possible gossip time under the model above. In some sense, first kind Frobenius graphs admit ‘perfect’ routing and gossiping schemes, and hence they are ‘perfect’ for interconnection networks as far as routing and gossiping are concerned.

Being studied extensively, circulant graphs (or undirected multi-loop networks [8] as used in theoretic computer science) have been recognized as strong candidates for interconnection networks. It is known that some circulant graphs are first kind Frobenius graphs. For instance,

in [20] the authors prove that all 6-valent circulant graphs with a given diameter and maximum possible order are Frobenius of the first kind. Because of the importance of circulant graphs (especially in the case of small valencies) in network design and very attractive properties of first kind Frobenius graphs with respect to routing and gossiping, the following problem arises naturally.

**Problem 1** *Classify all first kind Frobenius circulant graphs.*

In this paper we solve this problem in the case of valency four, and then we describe optimal routing and gossiping schemes for 4-valent first kind Frobenius circulant graphs. Let  $n \geq 5$  be an integer, and let  $1 \leq a, b \leq n - 1$  be distinct integers such that  $a, b \neq n/2$  and  $a + b \neq n$ . Let  $\mathbb{Z}_n$  be the additive group of integers modulo  $n$  and  $[x] \in \mathbb{Z}_n$  the residue class containing  $x$ . Then

$$DL_n(a, b) = \text{Cay}(\mathbb{Z}_n, S), \text{ where } S = \{[a], -[a], [b], -[b]\}$$

is a 4-valent circulant graph. It is connected if and only if  $\gcd(a, b, n) = 1$  (see e.g. [8, 21]). In the literature  $DL_n(a, b)$  is also called a double-loop network, justifying our notation, a double-loop fixed step graph [23], or a chordal ring of degree four [15]. As we will see in Lemma 5, we may assume without loss of generality that one of  $a, b$  is equal to 1.

A *complete rotation* [3, 9, 10] of a Cayley graph  $\text{Cay}(K, S)$  is a group automorphism of  $K$  which fixes  $S$  setwise and induces a cyclic permutation on  $S$ . A connected graph  $\Gamma$  is said to be *G-arc transitive* if  $G \leq \text{Aut}(\Gamma)$  is transitive on  $\text{Arc}(\Gamma)$ , the set of arcs of  $\Gamma$ . Let  $\mathbb{Z}_n^* = \{[m] : 0 < m < n, \gcd(m, n) = 1\}$  be the multiplicative group of units of ring  $\mathbb{Z}_n$ . The first result of this paper is the following theorem.

**Theorem 2** *Let  $n \geq 5$  be an integer. If  $n$  is even, then there exists no first kind Frobenius circulant graph of order  $n$  and valency four. If  $n$  is odd, then the following statements are equivalent:*

- (a) *there exists  $1 < h < n - 1$  such that  $DL_n(1, h)$  is a first kind Frobenius graph;*
- (b) *the quadratic congruence equation  $x^2 + 1 \equiv 0 \pmod{n}$  has a solution;*
- (c) *each prime factor of  $n$  is congruent to 1 modulo 4.*

*Moreover, if one of these occurs, then the following hold:*

- (d) *each solution  $h$  to  $x^2 + 1 \equiv 0 \pmod{n}$  gives rise to a first kind Frobenius circulant graph  $DL_n(1, h)$ , and vice versa, and in this case  $DL_n(1, h)$  is a  $\mathbb{Z}_n \rtimes H$ -arc transitive  $\mathbb{Z}_n \rtimes H$ -Frobenius graph which admits  $[h]$  and  $-[h]$  as complete rotations, where  $H = \langle [h] \rangle = \{[1], [h], [h^2], [h^3]\} = \{[1], [h], -[1], -[h]\} \leq \mathbb{Z}_n^*$ ;*
- (e) *there are exactly  $2^{l-1}$  pairwise non-isomorphic first kind Frobenius circulant graphs with order  $n$  and valency four, where  $l$  is the number of distinct prime factors of  $n$ , and each of them is isomorphic to  $DL_n(1, h)$  for some  $h$  as above.*

*In particular, for any prime  $p \equiv 1 \pmod{4}$  and integer  $e \geq 1$ , there is a unique first kind Frobenius circulant graph with order  $p^e$  and valency four.*

The equivalence of (b) and (c) above can be easily derived from known results in number theory. That  $DL_n(1, h)$  is  $\mathbb{Z}_n \rtimes H$ -arc transitive follows from a general result [25, Lemma 2.1]. The enumeration in (e) relies on known results on circulant CI-graphs (see [13] for a survey). Note that  $H$  (as a set) is identical to the connection set of  $DL_n(1, h)$ .

A routing of a graph  $\Gamma$  is  $G$ -arc transitive [14] if  $G \leq \text{Aut}(\Gamma)$  is transitive on  $\text{Arc}(\Gamma)$  and leaves the routing invariant. The next theorem summarizes routing and gossiping properties of first kind Frobenius circulant graphs of valency four. Note that the value of  $t(DL_n(1, h))$  is independent of  $h$  and that  $\sum_{i=0}^r x_i(x_i + 2i + 1)$  is another form of  $\sum_{u,v \in V(\Gamma)} d(u, v)/|E(\Gamma)|$ , where  $r, x_0, x_1, \dots, x_r$  will be defined in Section 3.

**Theorem 3** *Let  $n \geq 5$  be an integer with each prime factor congruent to 1 modulo 4. Let  $h$  be a solution to  $x^2 + 1 \equiv 0 \pmod n$  and  $H = \{[1], [h], -[1], -[h]\}$ . Then*

$$\pi(DL_n(1, h)) = 2\vec{\pi}(DL_n(1, h)) = 2\vec{\pi}_m(DL_n(1, h)) = \pi_m(DL_n(1, h)) = \sum_{i=0}^r x_i(x_i + 2i + 1) \quad (1)$$

$$t(DL_n(1, h)) = \frac{n-1}{4}. \quad (2)$$

Moreover, there exists a shortest path routing of  $DL_n(1, h)$  which is  $\mathbb{Z}_n \rtimes H$ -arc transitive, edge- and arc-uniform, and optimal for  $\pi, \vec{\pi}, \vec{\pi}_m$  and  $\pi_m$  simultaneously.

Furthermore, there exists an optimal gossiping scheme for  $DL_n(1, h)$  such that: (a) the message originating from any vertex is transmitted along shortest paths to other vertices; (b) for each vertex  $[w]$  of  $DL_n(1, h)$ , at any time  $t \geq 1$  precisely four arcs are used to transmit the message originating from  $[w]$ , and for  $t \geq 2$  these four arcs form a matching of  $DL_n(1, h)$ ; (c) at any time each arc of  $DL_n(1, h)$  is used exactly once for message transmission.

In general, such routing and gossiping schemes are not unique, and we give a systematic way of constructing them explicitly.

The existence of these routing and gossiping schemes and the formulae above are corollaries of Theorem 2 and some general results [25, Theorems 5.1 and 6.1] for any Frobenius graph of the first kind. In this paper we thus emphasize construction of routing and gossiping with the properties above. To this end we require detailed information about the  $H$ -orbits on  $\mathbb{Z}_n \setminus \{[0]\}$ , and this will be derived in Section 3. With such information we then obtain the promised schemes by specifying certain procedures in [25]. Due to the importance of circulant graphs, we feel that it is necessary to include such specifications for potential practical applications. As we will see in the last section, Theorem 2 implies that the unique 4-valent circulant graph with a given diameter and maximum possible order is a first kind Frobenius graph. For this graph we recover certain known results [15, 23] as consequences of Theorems 2 and 3.

The reader is referred to [6, 18] and [4] respectively for group- and graph-theoretic terminology used in the paper.

## 2 Proof of Theorem 2

It is well known (see e.g. [18, Section 5.7]) that  $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ . As the automorphism group of  $\mathbb{Z}_n$ ,  $\mathbb{Z}_n^*$  acts on  $\mathbb{Z}_n$  by usual multiplication:  $[x][m] = [xm]$ ,  $[m] \in \mathbb{Z}_n^*$ ,  $[x] \in \mathbb{Z}_n$ .  $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$  acts

on  $\mathbb{Z}_n$  in such a way that  $\mathbb{Z}_n$  acts by addition and  $\mathbb{Z}_n^*$  acts by multiplication. In other words,  $[x]^{([z],[m])} = [(x+z)m]$  for  $[x] \in \mathbb{Z}_n$  and  $([z],[m]) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ , where  $[z] \in \mathbb{Z}_n$  and  $[m] \in \mathbb{Z}_n^*$ . We identify  $\mathbb{Z}_n \rtimes \text{Aut}(\mathbb{Z}_n)$  with  $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$  in the following.

**Lemma 4** *A subgroup  $H$  of  $\mathbb{Z}_n^*$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$  if and only if  $[h-1] \in \mathbb{Z}_n^*$  for all  $[h] \in H \setminus \{[1]\}$ .*

**Proof**  $H$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\} \Leftrightarrow$  for any  $[x] \in \mathbb{Z}_n \setminus \{[0]\}$  and  $[h] \in H$ ,  $[hx] = [x]$  implies  $[h] = [1] \Leftrightarrow [(h-1)x] \neq [0]$  for any  $[x] \in \mathbb{Z}_n \setminus \{[0]\}$  and any  $[h] \in H \setminus \{[1]\} \Leftrightarrow \gcd(h-1, n) = 1$  for all  $[h] \in H \setminus \{[1]\} \Leftrightarrow [h-1] \in \mathbb{Z}_n^*$  for all  $[h] \in H \setminus \{[1]\}$ .

**Lemma 5** *Let  $n \geq 5$  be an integer. If  $DL_n(a, b)$  is a first kind Frobenius graph, then the following hold:*

- (a) *There exists a cyclic subgroup  $H$  of  $\mathbb{Z}_n^*$  with order four such that  $DL_n(a, b)$  is a  $\mathbb{Z}_n \rtimes H$ -Frobenius graph;*
- (b) *at least one of  $a, b$  is coprime to  $n$ , and there exists an integer  $b'$  with  $1 < b' < n-1$  and  $b' \neq n/2$  such that  $DL_n(a, b) \cong DL_n(1, b')$ .*

**Proof** Since  $DL_n(a, b)$  is a first kind Frobenius graph, there exists a Frobenius group  $G = \mathbb{Z}_n \rtimes H$  with Frobenius kernel  $\mathbb{Z}_n$  such that  $DL_n(a, b)$  is a first kind  $G$ -Frobenius graph. Hence  $S$  is an  $H$ -orbit (under the action of  $H$  on  $\mathbb{Z}_n$ ),  $H$  is regular on  $S = \{[a], -[a], [b], -[b]\}$  and semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ . Thus  $|H| = |S| = 4$ , and so either  $H \cong \mathbb{Z}_4$  or  $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Note that  $H$  is isomorphic to a subgroup of  $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$  and hence we may take  $H$  as a subgroup of  $\mathbb{Z}_n^*$ .

Since  $H$  is transitive on  $S$ , there exists an element  $[m] \in H$  such that  $[am] = [b]$ . Note that  $[m] \neq [1]$  as  $[a] \neq [b]$ . Since every element of  $\mathbb{Z}_2 \times \mathbb{Z}_2$  other than the identity is an involution, if  $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ , then  $[bm] = [a]$  and hence  $[(a+b)m] = [a+b]$ , which is a contradiction because  $[a+b] \neq [0]$ ,  $[m] \neq [1]$  and  $H$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ . Therefore,  $H \cong \mathbb{Z}_4$  and so  $H = \{[1], [h], [h^2], [h^3]\}$  for some  $[h] \in H$ .

Since  $DL_n(a, b)$  is a Frobenius graph, it must be connected and hence  $\gcd(a, b, n) = 1$ . We claim that at least one of  $a, b$  is coprime to  $n$ . Suppose otherwise, then since  $S$  is invariant under the action of  $H$ , we have  $[ha] = \pm[a]$  or  $\pm[b]$ . If  $[ha] = -[a]$ , then  $[h^2a] = -[ha] = [a]$  and hence  $H$  is intransitive on  $S$ , a contradiction. Note that  $\gcd(a, n) = d > 1$  since  $a$  is not coprime to  $n$  by our assumption. If  $[ha] = [b]$ , then since  $d \mid a$  and  $d \mid n$  we have  $d \mid b$ , which contradicts  $\gcd(a, b, n) = 1$ . Similarly,  $[ha] = -[b]$  can not happen. If  $[ha] = [a]$ , then since  $H$  is regular on  $S$  we must have  $[h] = [1]$  and so  $H = \{[1]\}$ , again a contradiction. Thus, we have proved that at least one of  $a, b$  is coprime to  $n$ . Without loss of generality we may assume  $\gcd(a, n) = 1$ . Then  $[a] \in \mathbb{Z}_n^*$  and hence  $DL_n(a, b) \cong DL_n(1, b')$  via the automorphism  $[a]$  of  $\mathbb{Z}_n$ , where  $[b'] = [a]^{-1}[b] \neq \pm[1]$  with  $[a]^{-1}$  the inverse of  $[a]$  in  $\mathbb{Z}_n^*$ . We may assume  $1 < b' < n-1$ . Since  $DL_n(a, b)$  has valency four, we have  $b' \neq n/2$ .  $\square$

**Proof of Theorem 2** Suppose  $DL_n(1, h)$  is a first kind Frobenius graph, where  $1 < h < n$  and  $h \neq n/2$ . Then by Lemma 5(a) there exists a cyclic subgroup  $H = \langle [h_0] \rangle$  of  $\mathbb{Z}_n^*$  with order four such that  $DL_n(1, h)$  is a  $\mathbb{Z}_n \rtimes H$ -Frobenius graph. Hence  $H$  is regular on  $S = \{[1], -[1], [h], -[h]\}$  and semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ . Since  $[1] \in S$ , the regularity of  $H$  on  $S$

implies  $S = H = \{[1], [h_0], [h_0]^2, [h_0]^3\}$ , and in particular  $-[1] \in H$ . Clearly,  $-[1] \neq [h_0]$ , and if  $-[1] = [h_0]^3$  then  $[1] = [h_0]^6 = [h_0]^2$  and so  $H = \{[1], -[1]\}$ , a contradiction. So the only possibility is that  $[h_0]^2 = -[1]$ , that is,  $h_0$  is a solution to  $x^2 + 1 \equiv 0 \pmod n$ . It follows that  $H = \{[1], -[1], [h_0], -[h_0]\} = S$ . We may assume  $[h_0] = [h]$  for otherwise we replace  $h$  by  $n - h$ . Hence  $h$  is a solution to  $x^2 + 1 \equiv 0 \pmod n$  and therefore (a) implies (b). Moreover, since  $H$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ , by Lemma 4 we should have  $[h^2 - 1] = [-2] \in \mathbb{Z}_n^*$ , which occurs only when  $n$  is odd. Thus, if  $n$  is even, then there exists no first kind Frobenius circulant graph of order  $n$  and valency four.

In the remainder of this proof we assume that  $n = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$  is odd, where  $p_1, p_2, \dots, p_l$  are distinct odd primes and  $e_1, e_2, \dots, e_l$  are positive integers. Suppose (b) holds and let  $h$  be a solution to  $x^2 + 1 \equiv 0 \pmod n$ . Then by the discussion in [16, Section 2.5]  $h$  is also a solution to the system of congruences  $x^2 + 1 \equiv 0 \pmod{p_i^{e_i}}$ ,  $1 \leq i \leq l$ . Hence each  $p_i$  is a divisor of  $h^2 + 1$ . It follows that none of  $p_i$ 's can be a divisor of  $h$ . Therefore,  $\gcd(h, n) = 1$  and so  $[h] \in \mathbb{Z}_n^*$ . Since  $h^2 \equiv -1 \pmod n$ , it follows that  $H = \langle [h] \rangle = \{[1], [h], [h]^2, [h]^3\} = \{[1], -[1], [h], -[h]\}$  is a cyclic subgroup of  $\mathbb{Z}_n^*$  of order four. Consider  $DL_n(1, h) = \text{Cay}(\mathbb{Z}_n, S)$ , where  $S = H$ . Clearly,  $H$  is regular on  $S$ . Since  $n$  is odd,  $[h^2 - 1] = [-2] \in \mathbb{Z}_n^*$ . If  $[h - 1] \notin \mathbb{Z}_n^*$ , then there exists some  $i$  such that  $p_i$  is a divisor of  $h - 1$ , and hence  $p_i$  is a divisor of  $h^2 - 1$ . Since  $p_i$  is a divisor of  $h^2 + 1$ , it follows that  $p_i$  is a divisor of 2, a contradiction. Hence we must have  $[h - 1] \in \mathbb{Z}_n^*$ . Similarly, one can show that  $[h^3 - 1] = [-h - 1] \in \mathbb{Z}_n^*$ . Therefore, by Lemma 4,  $H$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ . Consequently,  $\mathbb{Z}_n \rtimes H$  is a Frobenius group (see e.g. [17, pp.211]) and  $DL_n(1, h)$  is a first kind  $\mathbb{Z}_n \rtimes H$ -Frobenius graph. Thus, (b) implies (a).

For an integer  $m \geq 1$ , let  $N(m)$  denote the number of solutions to  $x^2 + 1 \equiv 0 \pmod m$ . Then  $N(n) = \prod_{i=1}^l N(p_i^{e_i})$  by [16, Theorem 2.18]. Since each  $p_i$  is odd, by [12, Proposition 4.2.3],  $N(p_i^{e_i}) \geq 1$  if and only if  $N(p_i) \geq 1$ , which is true if and only if  $p_i \equiv 1 \pmod 4$  ([16, Theorem 2.11]). Thus,  $N(n) \geq 1$  if and only if each prime factor of  $n$  is congruent to 1 modulo 4. That is, (b) and (c) are equivalent for odd integers  $n$ .

Suppose that one of (a)-(c) holds, so that each  $p_i$  is congruent to 1 modulo 4. The proof above shows that every solution  $h$  to  $x^2 + 1 \equiv 0 \pmod n$  gives rise to a first kind Frobenius circulant graph  $DL_n(1, h)$ , and vice versa, and in this case  $DL_n(1, h)$  is a  $\mathbb{Z}_n \rtimes H$ -Frobenius graph, where  $H = \langle [h] \rangle = \{[1], -[1], [h], -[h]\} \leq \mathbb{Z}_n^*$ . Clearly,  $[h]$  and  $-[h]$  are complete rotations of  $DL_n(1, h)$ . Also,  $\mathbb{Z}_n \rtimes H \leq \text{Aut}(DL_n(1, h))$  and  $\mathbb{Z}_n \rtimes H$  is transitive on the vertices of  $DL_n(1, h)$ . Let  $([x], [y])$  and  $([u], [v])$  be arcs of  $DL_n(1, h)$ . Then  $[x - y], [u - v] \in S = H$ . Since  $H$  is transitive on  $S$ , there exists  $[m] \in H$  such that  $[x - y][m] = [u - v]$ . Let  $[z] = [v][m]^{-1} - [y]$ , where  $[m]^{-1}$  is the inverse element of  $[m]$  in  $\mathbb{Z}_n^*$ , so that  $[(y + z)m] = [v]$ . Then  $([x], [y])^{([z], [m])} = ([x + z]m, [(y + z)m]) = ([x + z]m + (u - v), [(y + z)m]) = ([u], [v])$ . Therefore,  $DL_n(1, h)$  is  $\mathbb{Z}_n \rtimes H$ -arc transitive and (d) is established.

For each  $i$ , we have  $N(p_i^{e_i}) = N(p_i) = 2$ , where the first equality is from [12, Proposition 4.2.3] and the second one from [16, Corollary 2.28]. Hence  $N(n) = \prod_{i=1}^l N(p_i^{e_i}) = 2^l$ . By part (b) of Lemma 5, every first kind Frobenius circulant graph of order  $n$  and valency four is isomorphic to some  $DL_n(1, h)$ , where  $h$  is a solution to  $x^2 + 1 \equiv 0 \pmod n$ . Note that  $-h$  is also a solution to this congruence equation and it gives rise to the same graph. Since  $N(n) = 2^l$ , it follows that there are at most  $2^{l-1}$  pairwise non-isomorphic first kind Frobenius circulant graphs with order  $n$  and valency four. To establish (e) it remains to prove that, for distinct solutions  $h_1, h_2$  to  $x^2 + 1 \equiv 0 \pmod n$  such that  $h_1 \not\equiv \pm h_2 \pmod n$ , we have  $DL_n(1, h_1) \not\cong$

$DL_n(1, h_2)$ . In fact, if  $DL_n(1, h_1) \cong DL_n(1, h_2)$ , then since every cyclic group is a 4-CI group (see e.g. [13]), there exists  $[m] \in \mathbb{Z}_n^*$  such that  $S_1[m] = S_2$ , where  $S_1 = \{[1], -[1], [h_1], -[h_1]\}$  and  $S_2 = \{[1], -[1], [h_2], -[h_2]\}$ . From the proof above  $H_1 = \langle [h_1] \rangle = S_1$  and  $H_2 = \langle [h_2] \rangle = S_2$  are subgroups of  $\mathbb{Z}_n^*$ . Since  $[1] \in S_2$ , there exists  $[x] \in S_1$  such that  $[xm] = [1]$ , and this implies  $[m] \in H_1$ . Thus,  $S_2 = S_1[m] = H_1[m] = H_1 = S_1$ , which contradicts the assumption that  $h_1 \not\equiv \pm h_2 \pmod n$ .  $\square$

**Remark 6** Let  $n = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$  be as above. All solutions to  $x^2 + 1 \equiv 0 \pmod n$  can be computed by using known results in number theory. In fact, since  $p_i \equiv 1 \pmod 4$ , from the proof of [16, Theorem 2.11],  $\prod_{j=1}^{(p_i-1)/2} j \pmod{p_i}$  and  $p_i - \prod_{j=1}^{(p_i-1)/2} j \pmod{p_i}$  are the two solutions to  $x^2 + 1 \equiv 0 \pmod{p_i}$ . Based on these we obtain the two solutions to  $x^2 + 1 \equiv 0 \pmod{p_i^{e_i}}$  by applying the procedure in the proof of [12, Proposition 4.2.3]. Using the method in the proof of [16, Theorem 2.18], we then obtain all  $2^l$  solutions to  $x^2 + 1 \equiv 0 \pmod n$  and hence all  $2^{l-1}$  first kind Frobenius circulant graphs of order  $n$  and valency four.

### 3 Optimal routing and gossiping

Let  $n \geq 5$  be an integer with each prime factor congruent to 1 modulo 4, and let  $h$  be a solution to  $x^2 + 1 \equiv 0 \pmod n$ . Then  $h \neq n/2$ . Let  $\Gamma = DL_n(1, h)$ ,  $H = \langle [h] \rangle = \{[1], -[1], [h], -[h]\}$ , and let  $d$  be the diameter and  $(n_1, n_2, \dots, n_d)$  the type of  $\Gamma$ . Let  $\Gamma_i[u] = \{[v] \in \mathbb{Z}_n : d([u], [v]) = i\}$  for  $[u] \in \mathbb{Z}_n$  and  $1 \leq i \leq d$ , where  $d([u], [v])$  is the distance in  $\Gamma$  between  $[u]$  and  $[v]$ . Then  $\Gamma_i[0]$  is a union of  $n_i$   $H$ -orbits; in particular,  $\Gamma_1[0] = H$  (as a set) and  $n_1 = 1$ . Since by Theorem 2,  $H \leq \mathbb{Z}_n^*$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ , all  $H$ -orbits on  $\mathbb{Z}_n \setminus \{[0]\}$  contain four vertices of  $\Gamma$ .

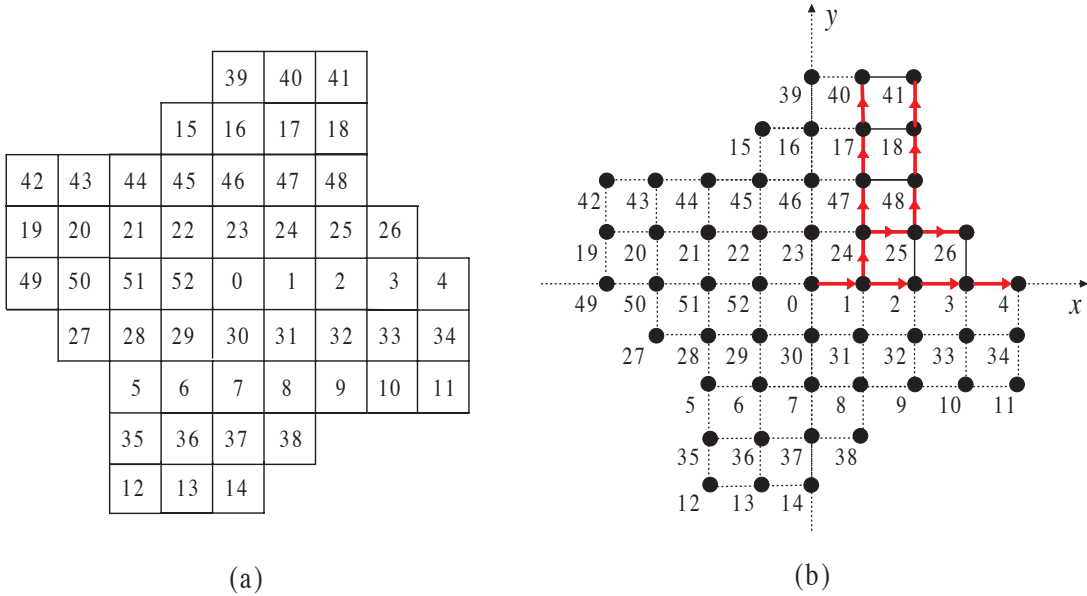


Figure 1: Geometric representations of  $DL_{53}(1, 23)$  by (a) a plane tessellation and (b) an integer lattice. For this graph,  $r = x_0 = 4, x_1 = 3, x_2 = x_3 = x_4 = 2$ ,  $X$  consists of those vertices connected by solid lines, and lines with arrows form the part  $T_0^1$  of a shortest path spanning tree  $T_0$  in the first quadrant.

Geometrically, we may represent  $\Gamma$  by a plane tessellation of squares [8, 22, 21] or integer lattice [24]. See Figure 1 for an illustration. Let  $\mathbb{Z}^2$  be the 2-dimensional integer lattice. Then each  $(x, y) \in \mathbb{Z}^2$  represents a vertex  $[x + yh]$  of  $\Gamma$ , and this defines a mapping from  $\mathbb{Z}^2$  to  $\mathbb{Z}_n$ . By the definition of  $\Gamma$ , for  $0 \leq v \leq n - 1$ , we have

$$d([0], [v]) = \min\{|x| + |y| : (x, y) \in \mathbb{Z}^2, v \equiv x + yh \pmod{n}\} \leq v.$$

Let  $r$  be the largest  $v$  such that  $d([0], [v]) = v$ . Since  $d([0], [1]) = 1$ ,  $r$  is well-defined. Since the  $H$ -orbit containing  $[v]$  is  $[v]H = \{[v], [vh], -[v], -[vh]\}$ ,  $r$  is also the largest  $v$  such that  $d([0], [vh]) = v$  ( $d([0], -[v]) = v$ ,  $d([0], -[vh]) = v$ , respectively). Hence  $1 \leq r \leq (n - 1)/4$ . Moreover, for  $0 \leq k \leq r$ , we have

$$d([0], [k]) = d([0], [kh]) = d([0], -[k]) = d([0], -[kh]) = k. \quad (3)$$

In fact, since  $H \leq \text{Aut}(\Gamma)$  fixes  $[0]$ , the four distances above must be equal. If  $d([0], [k]) \leq k - 1$ , then there exist  $(x, y) \in \mathbb{Z}^2$  such that  $k \equiv x + yh \pmod{n}$  and  $d([0], [k]) = |x| + |y| \leq k - 1$ . Thus  $r = k + (r - k) \equiv x + yh + (r - k) \pmod{n}$  and so  $r = d([0], [r]) \leq |x| + |y| + (r - k) \leq r - 1$ . This contradiction proves (3).

In general, for  $0 \leq k \leq r$  let  $x_k \geq 0$  be the largest integer such that  $d([0], [x_k + kh]) = x_k + k$ . Note that  $x_k$  is well-defined because of (3). Let

$$X = \{[j + kh] : 1 \leq j \leq x_k, 0 \leq k \leq r\}.$$

Since the  $H$ -orbit containing  $[j + kh] \in X$  is  $[j + kh]H = \{[j + kh], [-k + jh], [-j - kh], [k - jh]\}$ , the image of  $X$  under the action of  $H$  (namely  $\cup_{[j+kh] \in X} [j + kh]H$ ) is given by

$$XH = \{[j + kh], [-k + jh], [-j - kh], [k - jh] : 1 \leq j \leq x_k, 0 \leq k \leq r\}.$$

The following results can be verified easily and hence we omit their proofs.

**Lemma 7** *With the notation above, the following hold:*

- (a) for  $[j + kh] \in X$ ,  $d([0], [j + kh]) = d([0], [-k + jh]) = d([0], [-j - kh]) = d([0], [k - jh]) = j + k$ ;
- (b)  $(n - 1)/4 \geq r = x_0 \geq x_1 \geq \dots \geq x_r$ ;
- (c)  $XH = \mathbb{Z}_n \setminus \{[0]\}$  and each element of  $\mathbb{Z}_n \setminus \{[0]\}$  appears in  $XH$  exactly once;
- (d)  $d = \max\{x_k + k : 0 \leq k \leq r\}$ ,  $XH \subseteq \{[x + yh] : (x, y) \in \mathbb{Z}^2, |x| + |y| \leq d\}$ , and if  $d = x_{k^*} + k^*$  then  $x_k \leq x_{k^*} - (k - k^*)$  for  $0 \leq k \leq r$ ;
- (e) for  $1 \leq i \leq d$ ,  $n_i = |\{[j + kh] \in X : j + k = i\}|$  and  $\Gamma_i[0] = \cup_{[j+kh] \in X, j+k=i} [j + kh]H$ .

**Remark 8** (a)  $XH$  is an algebraic expression of the minimum distance diagram [8, 22, 21] of  $\Gamma$ . In the current situation this diagram is symmetric and the group  $H$  permutes the four parts of  $XH$  cyclically: The part in the first quadrant is  $X$ , and the parts in the other three quadrants are  $X[h]$ ,  $-X$ ,  $-X[h]$  successively. The lattice  $\mathbb{Z}^2$  is covered by copies of  $XH$  periodically, and  $XH$  induces a subgraph of  $\Gamma$  in which each ‘interior vertex’ is fully connected to four vertices of  $\Gamma$ .



(b) In general, it is hard to give a formula for  $x_k$  in terms of  $n$  and  $h$ ,  $0 \leq k \leq r$ , because for otherwise we could get a formula for the diameter of  $\Gamma$ . The latter task is very difficult as shown in the literature [8, 24]. The minimum distance diagram  $XH$  can be constructed [22] by labelling the vertices  $(x, y) \in \mathbb{Z}^2$  by  $|x| + |y|$  in increasing order of  $|x| + |y|$ , discarding repeated labels, until all integers  $0, 1, \dots, n-1$  are present. We obtain all  $x_k$  easily once we find the minimum distance diagram.

(c) In [24] an  $O(\log n)$  algorithm for computing the diameter of any circulant graph of valency four was given. This can be used to compute the diameter  $d$  of  $\Gamma$ .

Now we construct a spanning tree  $T_0$  of  $\Gamma$  rooted at  $[0]$  by using  $XH$ . The branch  $T_0^1$  of  $T_0$  in the first quadrant can be chosen as any subtree of  $\Gamma$  with vertex set  $X \cup \{[0]\}$  and containing the edge between  $[0]$  and  $[1]$  such that, for  $1 \leq i < d$ , each vertex in  $\Gamma_{i+1}[0] \cap X$  is adjacent to exactly one vertex in  $\Gamma_i[0] \cap X$ . To obtain the branches of  $T_0$  in the other three quadrants we rotate  $T_0^1$  by  $90^\circ, 180^\circ, 270^\circ$  respectively. In other words, these branches have vertex sets  $X[h] \cup \{[0]\}$ ,  $-X \cup \{[0]\}$ ,  $-X[h] \cup \{[0]\}$  and edges  $\{[uh], [vh]\}$ ,  $\{-[u], -[v]\}$ ,  $\{-[uh], -[vh]\}$  respectively with  $\{[u], [v]\}$  running over all edges of  $T_0^1$ . It is clear that  $T_0$  is a *shortest path spanning tree* of  $\Gamma$  with root  $[0]$ , that is, the unique path in  $T_0$  between  $[0]$  and any vertex is a shortest path in  $\Gamma$ . Consequently, for  $0 \leq i \leq d$ , the set  $T_0(i)$  of vertices distant  $i$  apart from  $[0]$  in  $T_0$  is identical to  $\Gamma_i[0]$ . Let  $A_{1,1}$  be the set of four arcs from  $[0]$  to  $\Gamma_1[0]$ , namely  $A_{1,1} = \{([0], [1]), ([0], [h]), ([0], -[1]), ([0], -[h])\}$ . For  $0 \leq i < d$ , since  $|\Gamma_{i+1}[0] \cap X| = n_{i+1}$ , we may denote the vertices in  $\Gamma_{i+1}[0] \cap X$  by  $[v_{i+1,j}]$ ,  $1 \leq j \leq n_{i+1}$ ; then for each  $1 \leq j \leq n_{i+1}$  let  $A_{i+1,j}$  be the image of the unique arc of  $T_0$  from a vertex of  $\Gamma_i[0] \cap X$  to  $[v_{i+1,j}]$  under the action of  $H$ . Thus the set of arcs of  $T_0$  from  $T_0(i)$  to  $T_0(i+1)$  is  $\cup_{1 \leq j \leq n_{i+1}} A_{i+1,j}$ . Since  $H$  is semiregular on  $\mathbb{Z}_n \setminus \{[0]\}$ , for  $1 \leq i < d$  and  $1 \leq j \leq n_{i+1}$ ,  $A_{i+1,j}$  is a matching of four arcs.

Given  $[u] \in \mathbb{Z}_n$ ,  $W \subseteq \mathbb{Z}_n$  and  $A \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ , denote  $W + [u] = \{[w + u] : [w] \in W\}$  and  $A + [u] = \{([x + u], [y + u]) : ([x], [y]) \in A\}$ . Define  $T_u$  to be the tree with vertex set  $\mathbb{Z}_n$  and arc set  $\text{Arc}(T_0) + [u]$ , that is,  $T_u$  is obtained from  $T_0$  by translation by  $[u]$ . Since  $\mathbb{Z}_n$  acts on itself (by translation) as a group of automorphisms of  $\Gamma$ ,  $T_u$  is a shortest path spanning tree of  $\Gamma$  with root  $[u]$ . Let

$$\mathcal{P} = \{P_{uv} : [u], [v] \in \mathbb{Z}_n, [u] \neq [v]\} \quad (4)$$

where  $P_{uv}$  is the unique path in  $T_u$  from  $[u]$  to  $[v]$ . The following algorithm gives the promised optimal gossiping scheme as we will see soon.

**Algorithm 9** Let  $M_u$  denote the message originating at  $[u] \in \mathbb{Z}_n$ .

**Phase 1:** Initially,  $M_u$  is transmitted from  $[u]$  to  $T_0(1) + [u]$  ( $= H + [u]$ ) along the four arcs of  $A_{1,1} + [u]$ , and this is carried out for all  $[u] \in \mathbb{Z}_n$  simultaneously.

**Phase  $i+1$ :** Do the following for  $i = 1, 2, \dots, d-1$  successively: for  $j = 1, 2, \dots, n_{i+1}$ , in the  $j$ th step of the  $(i+1)$ th phase, for all  $[u] \in \mathbb{Z}_n$  transmit  $M_u$  from  $T_0(i) + [u]$  to  $T_0(i+1) + [u]$  along the four arcs of  $A_{i+1,j} + [u]$  at the same time step.

**Proof of Theorem 3** Since each  $T_u$  is a shortest path spanning tree,  $\mathcal{P}$  as defined in (4) is a shortest path routing of  $\Gamma$ . Since  $T_0$  is invariant under  $H$ ,  $\mathbb{Z}_n \times H$  leaves  $\{T_u : [u] \in \mathbb{Z}_n\}$  and hence  $\mathcal{P}$  invariant. Since  $\Gamma$  is  $\mathbb{Z}_n \times H$ -arc transitive (Theorem 2(d)),  $\mathcal{P}$  is a  $\mathbb{Z}_n \times H$ -arc transitive routing. Thus,  $\mathcal{P}$  is arc- and hence edge-uniform. Consequently,  $\pi(\Gamma) = 2\overline{\pi}(\Gamma) = 2\overline{\pi}_m(\Gamma) =$

$\pi_m(\Gamma)$  and  $\mathcal{P}$  is optimal for the four indices simultaneously. Moreover, by Lemma 7 we have  $\pi(\Gamma) = \sum_{[u],[v] \in \mathbb{Z}_n} d([u],[v])/|E(\Gamma)| = 4n \sum_{k=0}^r \sum_{j=1}^{x_k} (j+k)/2n = \sum_{k=0}^r x_k(x_k+2k+1)$ .

Clearly,  $\{A_{1,1} + [u] : [u] \in \mathbb{Z}_n\}$  is a partition of  $\text{Arc}(\Gamma)$ . For  $1 \leq i < d, 1 \leq j \leq n_{i+1}$ , since  $\Gamma$  is  $\mathbb{Z}_n \rtimes H$ -arc transitive and  $A_{i+1,j}$  is invariant under  $H$ , each arc of  $\text{Arc}(\Gamma)$  is contained in at least one  $A_{i+1,j} + [u]$ ,  $[u] \in \mathbb{Z}_n$ . Since  $\sum_{[u] \in \mathbb{Z}_n} |A_{i+1,j} + [u]| = 4n = |\text{Arc}(\Gamma)|$ , it follows that  $\{A_{i+1,j} + [u] : [u] \in \mathbb{Z}_n\}$  is a partition of  $\text{Arc}(\Gamma)$ . Hence Algorithm 9 is a gossiping scheme such that at any time each arc is used exactly once. Clearly, it requires  $|X| = (n-1)/4$  time steps. However,  $t(\Gamma) \geq (n-1)/4$ , because  $n-1$  messages are to be sent to  $[0]$ , and at any time  $[0]$  can process at most four messages. Therefore,  $t(\Gamma) = (n-1)/4$  and Algorithm 9 gives an optimal gossiping scheme. Obviously, it has the features described in (a)-(c) of Theorem 3.  $\square$

## 4 Concluding remarks

It is known [21] that the maximum order of a connected 4-valent circulant graph with a given diameter  $d \geq 2$  is  $n_d = 2d^2 + 2d + 1$ . Moreover, up to isomorphism there is a unique connected 4-valent circulant graph [21] with diameter  $d$  and order  $n_d$ , namely  $DL_{n_d}(1, 2d+1)$ . (In fact, for any such graph  $DL_{n_d}(a, b)$ , we have  $a(d+1) - bd \equiv 0, ad + b(d+1) \equiv 0 \pmod{n_d}$  by [21, Eq. (3)] and so  $a \equiv b(2d+1) \pmod{n_d}$ . Thus, since  $DL_{n_d}(a, b)$  is connected, we have  $\gcd(b, n_d) = \gcd(a, b, n_d) = 1$ . Hence  $[b] \in \mathbb{Z}_{n_d}^*$  and  $DL_{n_d}(a, b) \cong DL_{n_d}(b(2d+1), b) \cong DL_{n_d}(1, 2d+1)$ .) From the discussion in [21],  $DL_{n_d}(1, 2d+1)$  has type  $(1, 2, \dots, d)$ , and hence  $r = d$  and  $x_k = d - k$  for  $0 \leq k \leq d$ . Since  $2d+1$  is a solution to  $x^2 + 1 \equiv 0 \pmod{n_d}$ , we obtain the following corollary of Theorems 2 and 3.

**Corollary 10** *Let  $d \geq 2$  be an integer, and let  $\Gamma = DL_{n_d}(1, 2d+1)$  be the unique connected 4-valent circulant graph of diameter  $d$  and maximum order  $n_d = 2d^2 + 2d + 1$ . Then  $\Gamma$  is a  $\mathbb{Z}_{n_d} \rtimes H(d)$ -arc transitive  $\mathbb{Z}_{n_d} \rtimes H(d)$ -Frobenius graph, where  $H(d) = \{[1], [2d+1], -[1], -[2d+1]\}$ , and*

$$\pi(\Gamma) = 2\vec{\pi}(\Gamma) = 2\vec{\pi}_m(\Gamma) = \pi_m(\Gamma) = \frac{d(d+1)(2d+1)}{3}$$

$$t(\Gamma) = \frac{d(d+1)}{2}.$$

Moreover, we can give explicitly optimal routing and gossiping schemes (not unique) for  $\Gamma$  with the properties described in Theorem 3.

That  $\vec{\pi}(DL_{n_d}(1, 2d+1)) = d(d+1)(2d+1)/6$  was obtained in [15] by pure combinatorial arguments. Here we recovered this formula as a special case of a general result. Moreover, instead of giving only one specific optimal routing [15], by choosing different shortest path spanning trees  $T_0$  and using the algorithms in the previous section we can give a number of optimal routing and gossiping schemes for  $DL_{n_d}(1, 2d+1)$ . (An example of  $T_0$  is given in Figure 2.) Furthermore, each  $T_0$  gives rise to a near optimal broadcasting scheme: at time  $t = 1, 2, 3, 4$  send the message at  $[0]$  to  $[1], [h], -[1], -[h]$  via the arcs of  $A_{1,1}$  successively; inductively, since  $n_i = n_{i-1} + 1$ , assume without loss of generality that  $A_{i,1}, A_{i,2}$  are joined to the same  $H(d)$ -orbit in  $T_0(i-1)$  ( $1 < i \leq d$ ); after all vertices in  $T_0(i)$  have received the message, for  $i = 2, \dots, d$  at time  $i+3$  transmit the message along the arcs of  $A_{i,1}, A_{i-1,2}, \dots, A_{i-1,i-1}$  simultaneously,

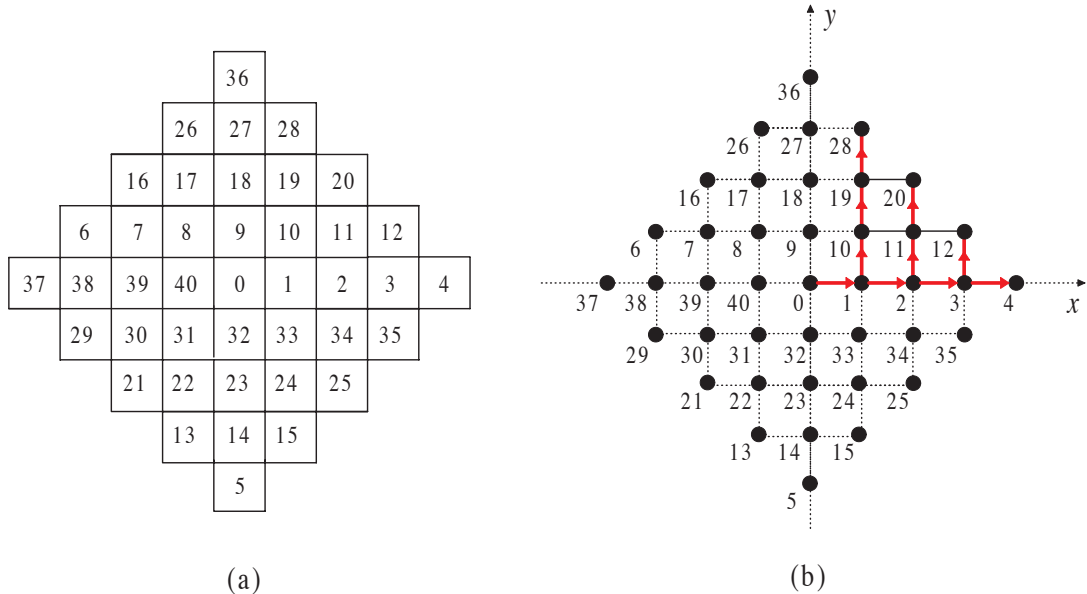


Figure 2: Part of a shortest path spanning tree of  $DL_{41}(1,9)$  in the first quadrant.

and at time  $d + 4$  send the message along the arcs of  $A_{d,2}, \dots, A_{d,d}$  simultaneously. This is a broadcasting scheme which requires  $d + 4$  time steps. It is near optimal since by [23] the minimum broadcasting time is  $d + 2$ .

Besides the ‘optimal’ double-loop networks  $DL_{n_d}(1, 2d + 1)$  above, there are other first kind Frobenius circulant graphs of valency four for which we can describe optimal routing and gossiping schemes explicitly. Consider  $\Gamma_m = DL_n(1, 2m)$  for example, where  $m \geq 1$  and  $n = 4m^2 + 1$ . Since  $2m$  is a solution to  $x^2 + 1 \equiv 0 \pmod n$ , by Theorem 2,  $\Gamma_m$  is a  $\mathbb{Z}_n \rtimes H$ -arc transitive  $\mathbb{Z}_n \rtimes H$ -Frobenius graph, where  $H = \{[1], [2m], -[1], -[2m]\}$ . For this graph we can easily find out  $r, x_0, x_1, \dots, x_r$  and hence give explicitly optimal routing and gossiping schemes by invoking the algorithms in the previous section.

The following problems arise naturally from our study in this paper. Note that problem (a) is different from the one of determining the minimum diameter among all 4-valent circulant graphs of order  $n$ , the latter being solved in [5].

**Problem 11** *Given an integer  $n \geq 5$  with each of its prime factors congruent to 1 modulo 4, determine (a) the minimum diameter of  $DL_n(1, h)$ , and (b) the minimum edge-forwarding index of  $DL_n(1, h)$ , for  $h$  running over all solutions to  $x^2 + 1 \equiv 0 \pmod n$ .*

**Acknowledgments** Alison Thomson was supported by a Postgraduate Award of the Australian Government. Sanming Zhou was supported by a Discovery Project Grant of the Australian Research Council.

## References

- [1] Sheldon B. Akers and Balakrishnan Krishnamurthy, A group-theoretic model for symmetric interconnection networks, *IEEE Trans. Comput.* **38** (1989), no. 4, 555-566.

- [2] Fred Annexstein, Marc Baumslag and Arnold Rosenberg, Group action graphs and parallel architectures, *SIAM J. Comput.* **19** (1990), no. 3, 544-569.
- [3] Jean-Claude Bermond, Takako Kodate and Stéphane Pérennes, Gossiping in Cayley graphs by packets, in: 8th Franco-Japanese and 4th Franco-Chinese Conf. Combin. Comput. Sci. (Brest, July 1995), *Lecture Notes in Computer Science*, **1120**, Springer-Verlag, 1996, pp.301-315.
- [4] Norman Biggs, *Algebraic Graph Theory (second edition)*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1993.
- [5] Francis T. Boesch and Jhing Fa Wang, Reliable circulant networks with minimum transmission delay, *IEEE Trans. Circuits Syst.* **32** (1985), 1286-1291.
- [6] John D. Dixon and Brian Mortimer, *Permutation Groups*, Springer, New York, 1996.
- [7] Xin Gui Fang, Cai Heng Li and Cheryl E. Praeger, On orbital regular graphs and Frobenius graphs, *Discrete Math.* **182** (1998), 85-99.
- [8] F. K. Hwang, A survey on multi-loop networks, *Theoret. Comput. Sci.* **299** (2003), 107-121.
- [9] Marie-Claude Heydemann, Cayley graphs and interconnection networks, in: G. Hahn and G. Sabidussi eds., *Graph Symmetry*, Kluwer Academic Publishing, Dordrecht, 1997, pp.167-224.
- [10] Marie-Claude Heydemann, Nausica Marlin and Stéphane Pérennes, Complete rotations in Cayley graphs, *Europ. J. Combinatorics* **22** (2001), 179-196.
- [11] Marie-Claude Heydemann, J.-C. Meyer and D. Sotteau, On forwarding indices of networks, *Discrete Applied Math.* **23** (1989), 103-123.
- [12] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982.
- [13] Cai Heng Li, On isomorphisms of finite Cayley graphs – a survey, *Discrete Math.* **256** (1-2) (2002), 301-334.
- [14] Tim Khoon Lim and Cheryl E. Praeger, Finding optimal routings in Hamming graphs, *Europ. J. Combinatorics* **23** (2002), 1033-1041.
- [15] L. Narayanan, J. Opatrny and D. Sotteau, All-to-all optical routing in chordal rings of degree 4, *Algorithmica* **31** (2) (2001), 155-178.
- [16] Ivan Niven and Herbert S. Zuckerman, *An introduction to the theory of numbers*, John Wiley & Sons, New York, 1980.
- [17] John S. Rose, *A Course on Group Theory*, Cambridge University Press, Cambridge, 1978.
- [18] W. R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
- [19] Patrick Solé, The edge-forwarding index of orbital regular graphs, *Discrete Math.* **130** (1994), no. 1-3, 171-176.
- [20] Alison Thomson and Sanming Zhou, Gossiping and routing in undirected triple-loop networks, submitted.
- [21] J. L. A. Yebra, M. A. Fiol, P. Morillo and I. Alegre, The diameter of undirected graphs associated to plane tessellations, *Ars Combinatoria* **20-B** (1985), 159-171.
- [22] C. K. Wong and Don Coppersmith, A combinatorial problem related to multimodule memory organizations, *J. Assoc. Comp. Mach.* **21** (3) (1974), 392-402.
- [23] M. Zaragoza, A. L. Liestman and J. Opatrny, Network properties of double and triple fixed step graphs, *Intern. J. Foundations of Com. Sci.* **9** (1998), 57-76.
- [24] Janez Žerovnik and Tomaž Pisanski, Computing the diameter in multi-loop networks, *J. Algorithms* **14** (1993), 226-243.
- [25] Sanming Zhou, A class of arc-transitive Cayley graphs as models for interconnection networks, submitted.