Discrete Mathematics and Theoretical Computer Science DMTCS vol. **14:2**, 2012, 173–188

On 4-valent Frobenius circulant graphs

Sanming Zhou[†]

Department of Mathematics and Statistics, The University of Melbourne, Parkville, VIC 3010, Australia

received 17th August 2011, revised 16th September 2012, accepted 20th October 2012.

A 4-valent first-kind Frobenius circulant graph is a connected Cayley graph $DL_n(1, h) = \mathrm{Cay}(\mathbb{Z}_n, H)$ on the additive group of integers modulo n, where each prime factor of n is congruent to 1 modulo 4 and $H = \{[1], [h], -[1], -[h]\}$ with h a solution to the congruence equation $x^2 + 1 \equiv 0 \pmod n$. In [A. Thomson and S. Zhou, Frobenius circulant graphs of valency four, J. Austral. Math. Soc. 85 (2008), 269–282] it was proved that such graphs admit 'perfect' routing and gossiping schemes in some sense, making them attractive candidates for modelling interconnection networks. In the present paper we prove that $DL_n(1, h)$ has the smallest possible broadcasting time, namely its diameter plus two, and we explicitly give an optimal broadcasting in $DL_n(1, h)$. Using number theory we prove that it is possible to recursively construct larger 4-valent first-kind Frobenius circulants from smaller ones, and we give a methodology for such a construction. These and existing results suggest that, among all 4-valent circulant graphs, 4-valent first-kind Frobenius circulants are extremely efficient in terms of routing, gossiping, broadcasting and recursive construction.

Keywords: Circulant graph; double-loop network; Gaussian network; Frobenius graph; broadcasting

1 Introduction

Let $n \geq 5$ be an integer whose prime factors are all congruent to 1 modulo 4. Then the congruence equation

$$x^2 + 1 \equiv 0 \bmod n \tag{1}$$

is solvable (see e.g. [14, 15]). For a solution h to this equation, let

$$H = \{[1], [h], -[1], -[h]\}, \tag{2}$$

where for an integer x, $[x]$ denotes the residue class of x modulo n. Define $DL_n(1, h)$ to be the circulant graph with vertex set $\mathbb{Z}_n$ such that $[x], [y] \in \mathbb{Z}_n$ are adjacent if and only if $[x-y] \in H$. We call $DL_n(1, h)$ a *4-valent first-kind Frobenius circulant graph* [18, 21] of order n. It is known [18, Theorem 2] that, for a fixed $n = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ such that $p_1, p_2, \ldots, p_l \equiv 1 \pmod 4$, where $p_1, p_2, \ldots, p_l$ are distinct prime factors of n and $e_1, e_2, \ldots, e_l \geq 1$, there are precisely 2^{l-1} pairwise non-isomorphic 4-valent first-kind

[†]Email: `smzhou@ms.unimelb.edu.au`

Frobenius circulant graphs of order n. We remark that, if h is a solution to (1), then so is $-h$, and h and $-h$ give rise to the same graph $DL_n(1, h)$.

The family of 4-valent first-kind Frobenius circulants was introduced in [18] in the context of optimal network design, and it was a subclass of a much larger class [3, 16, 21] of arc-transitive graphs, called the first-kind Frobenius graphs (see the next section for definition). The importance of such graphs lies in that they admit 'perfect' routing and gossiping schemes under the store-and-forward, all-port and full-duplex model (see [21] for detail). In the special case of 4-valent first-kind Frobenius circulants, this means that $DL_n(1, h)$ achieves the smallest possible edge-forwarding index and admits a shortest path routing which is optimal for the edge, arc, minimal-edge and minimal-arc forwarding indices [6] simultaneously. Moreover, under the store-and-forward, all-port and full-duplex model, $DL_n(1, h)$ has the smallest possible gossiping time and admits an optimal gossiping scheme under which messages are always transmitted along shortest paths, and at any time every arc is used exactly once for message transmission. (See [18, Theorem 3] for detail.) Because of these 4-valent first-kind Frobenius circulants are strong candidates for modelling interconnection networks. Such graphs are also useful in coding theory, and they were studied independently in [12] from a coding-theoretic point of view by using the language of Gaussian integers. Combining [12, Theorem 4] and the discussion in [17], it follows that the family of 4-valent first-kind Frobenius circulants is precisely the family of Gaussian graphs [12, Definition 3] of odd orders (see Lemma 5 and Remark 6).

The purpose of this paper is to study broadcasting in and recursive construction of 4-valent first-kind Frobenius circulants. We prove that such a graph achieves the smallest possible broadcasting time, namely its diameter plus two (Theorem 4). With the help of number theory we prove that it is possible to recursively construct larger 4-valent first-kind Frobenius circulants from smaller ones, and we give a methodology for such a construction (Section 4). These results make 4-valent first-kind Frobenius circulants even more attractive for modelling interconnection networks, besides their applications in coding theory. There is a long history in studying 4-valent circulants (also called double-loop networks) as models for networks; see e.g. [1, 8, 9] for surveys. The results in this paper and [18] suggests that, among all 4-valent circulants, 4-valent first-kind Frobenius circulants are exceedingly efficient in terms of routing, gossiping, broadcasting and recursive construction.

The reader is referred to [2] for group-theoretic terminology used in this paper.

2 Preliminaries

In this section we collect a few results on 4-valent first-kind Frobenius circulants that will be used in later sections.

Given a group X with identity element 1 and a subset $S \subseteq X \setminus \{1\}$ such that $s^{-1} \in S$ for every $s \in S$, the *Cayley graph* $\mathrm{Cay}(X, S)$ is defined to have vertex set X such that $x, y \in X$ are adjacent if and only if $xy^{-1} \in S$.

A Frobenius group is a transitive permutation group with the property that there are nonidentity elements fixing one point but only the identity element can fix two points. It is well known [2] that a finite Frobenius group is a semidirect product $K \rtimes H$, where K is a nilpotent normal subgroup, and we may think of $K \rtimes H$ as acting on K in such a way that K acts on K by right multiplication and H acts on K by conjugation. A *first-kind* $K \rtimes H$*-Frobenius graph* is defined [3, 21] as a Cayley graph $\mathrm{Cay}(K, a^H)$ on K, for some $a \in K$ such that $\langle a^H \rangle = K$, where a^H is the H-orbit containing a and either H is of even order or a is an involution. There is another class of graphs, called the second-kind Frobenius graphs [3], associated with finite Frobenius groups. The reader is referred to [4] for gossiping and routing properties of second-kind Frobenius graphs.

Let $\mathbb{Z}_n^* = \{[u] : 1 \le u \le n-1, \gcd(n,u) = 1\}$ be the multiplicative group of units of ring $\mathbb{Z}_n$. Then $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ and $\mathbb{Z}_n^*$ acts on $\mathbb{Z}_n$ by the usual multiplication: $[x][u] = [xu]$, $[x] \in \mathbb{Z}_n$, $[u] \in \mathbb{Z}_n^*$. The semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ acts on $\mathbb{Z}_n$ such that $[x]^{([y],[u])} = [(x+y)u]$ for $[x],[y] \in \mathbb{Z}_n$ and $[u] \in \mathbb{Z}_n^*$. We use $[u]^{-1}$ to denote the inverse element of $[u]$ in $\mathbb{Z}_n^*$. The operation of $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ is defined by $([x_1],[u_1])([x_2],[u_2]) = ([x_1] + [x_2][u_1]^{-1}, [u_1u_2])$ for $([x_1],[u_1]), ([x_2],[u_2]) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. Thus the inverse element of $([x],[u])$ in $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ is $(-[xu],[u]^{-1})$.

A graph G is called X*-arc-transitive* if X is a group of automorphisms of G such that any arc of G can be permuted to any other arc of G by an element of X, where an *arc* is an ordered pair of adjacent vertices.

Lemma 1 ([18]) *Let $n \ge 5$ be an integer all of whose prime factors are congruent to 1 modulo 4. Let h be a solution to (1) and H be as given in (2). Then $H = \langle [h] \rangle$ is a cyclic subgroup of $\mathbb{Z}_n^*$, $\mathbb{Z}_n \rtimes H$ is a Frobenius group, and $DL_n(1,h)$ is a $\mathbb{Z}_n \rtimes H$-arc-transitive first-kind $\mathbb{Z}_n \rtimes H$-Frobenius graph.*

In fact, by (1), $\gcd(h,n) = 1$ and $[h]^2 = -[1]$. Hence $\langle [h] \rangle = \{[1],[h],[h]^2,[h]^3\} = H \le \mathbb{Z}_n^*$. The last two statements in the lemma follow from [18, Theorem 2].

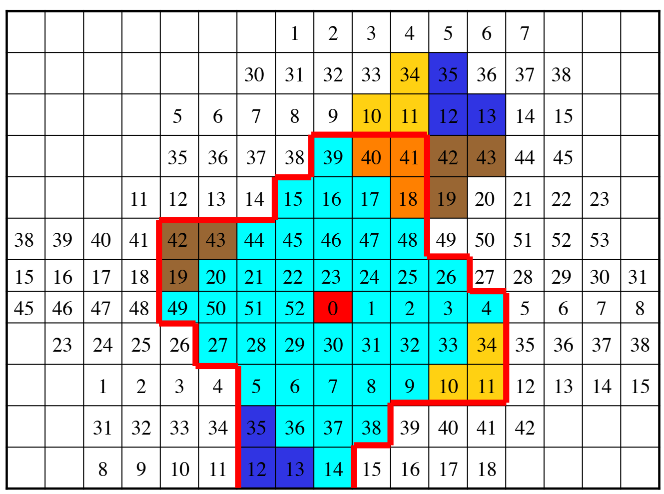

Fig. 1: Plane tessellation of $DL_{53}(1,23)$. The area bounded by the red lines is the minimum distance diagram $AH \cup \{[0]\}$, where $A = \{[1],[2],[3],[4],[24],[25],[26],[47],[48],[17],[18],[40],[41]\}$ is the part of AH in the first quadrant. The other three parts $A[h], -A, -A[h]$ of AH are obtained by rotating A about the origin by $90^\circ, 180^\circ, 270^\circ$ respectively. For this graph we have $d = 6, r = x_0 = 4, x_1 = 3, x_2 = x_3 = x_4 = 2, a = 2, b = 7$ and $n = 53 = 2^2 + 7^2$.

We may represent $DL_n(1,h)$ by a plane tessellation of squares [9, 19, 20] such that the square with coordinates (x,y) represents the vertex $[x+yh]$ of $DL_n(1,h)$ (see Figure 1). Thus the squares adjacent to $[x+yh]$ represent $[x+1+yh]$ (right), $[x-1+yh]$ (left), $[x+(y+1)h]$ (above) and $[x+(y-1)h]$ (below), respectively. Denote by $d([x],[y])$ the distance in $DL_n(1,h)$ between $[x]$ and $[y]$. Define [18]

$$r = \max\{x \geq 0 : d([0],[x]) = x\}.$$

For $0 \leq i \leq r$, define [18]

$$x_i = \max\{x \geq 0 : d([0],[x+ih]) = x+i\}.$$

Note that $x_0 = r$. Let

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

The image of A under the action of H is given by

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

Equivalently, AH intersects with the four quadrants at $A, A[h], -A, -A[h]$, respectively, and H permutes these four parts cyclically (see Figure 1), where $A[h] = \{[j+kh][h] : [j+kh] \in A\}$, $-A = \{[-j-kh] : [j+kh] \in A\}$ and $-A[h] = \{[-j-kh][h] : [j+kh] \in A\}$. (Note that $[j+kh][h] = [-k+jh]$ and $[-j-kh][h] = [k-jh]$ by (1).) $AH \cup \{[0]\}$ is an algebraic expression [18] of the minimum distance diagram [9, 19, 20] of $DL_n(1,h)$ as shown by the following lemma.

Lemma 2 ([18, Lemma 7]) *With the notation above, the following hold:*

(a) for $[j+kh] \in A$, $d([0],[j+kh]) = d([0],[-k+jh]) = d([0],[-j-kh]) = d([0],[k-jh]) = j+k$;

(b) the diameter d *of* $DL_n(1,h)$ *is given by* $d = \max\{x_k + k : 0 \leq k \leq r\}$;

(c) $AH = \mathbb{Z}_n \setminus \{[0]\}$ *and each element of* $\mathbb{Z}_n \setminus \{[0]\}$ *appears exactly once in* AH.

It is well known (e.g. [15, Corollary 6.8.2]) that the Diophantine equation

$$x^2 + y^2 = n \tag{3}$$

is solvable if and only if the canonical factorization of n into primes contains no factor p^e with e odd and $p \equiv 3 \pmod 4$. An integral solution (a,b) to (3) is called *primitive* if $\gcd(a,b) = 1$. It is known [15, Theorem 6.4] that every nonnegative primitive solution (a,b) of (3) determines a unique solution h of (1) such that $ah \equiv b \pmod n$, and different nonnegative primitive solutions determine different h modulo n. Conversely, if h is a solution of (1), then there is [15, Theorem 6.5] a nonnegative primitive solution (a,b) of (3) such that $ah \equiv b \pmod n$. Obviously, for such (a,b) we have $\gcd(a,n) = \gcd(b,n) = 1$ and the mapping $[x] \mapsto [ax], [x] \in \mathbb{Z}_n$ is an isomorphism from $DL_n(1,h)$ to $DL_n(a,b)$, the latter being the circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ with $S = \{[a],[b],-[a],-[b]\}$.

Lemma 3 ([12, Theorem 6], see also [17]) *Let $n \geq 5$ be an integer all of whose prime factors are congruent to 1 modulo 4. Let h be a solution to (1). Let $0 < a < b$ be the unique primitive solution of (3) such that $ah \equiv b \pmod{n}$. Then*

$$r = (a + b - 1)/2 \tag{4}$$

and, for $0 \leq i \leq r$,

$$x_i = \max\{r - i, r - a\}. \tag{5}$$

In particular, the diameter of $DL_n(1, h)$ is given by

$$d = x_r + r = b - 1.$$

3 Broadcasting time

A common process in communication networks is to disseminate a message from a specific *source vertex* to all other vertices in such a way that in each time step any vertex who has received the message already can retransmit it to at most one of its neighbours. This process is called *broadcasting*, and the minimum number of time steps required is denoted by $b(G, u)$ if G is the network and u is the source vertex. The *broadcasting time* [7] of G, denoted by $b(G)$, is defined to be the maximum among $b(G, u)$ for u running over $V(G)$. In general, it is difficult to determine $b(G)$. See [7, Section 5.2] for a survey.

The maximum order of a connected 4-valent circulant graph with a given diameter $d \geq 2$ is $n_d = 2d^2 + 2d + 1$ [20], and up to isomorphism $DL_{n_d}(1, 2d + 1)$ is the unique connected 4-valent circulant graph [20] with diameter d and order n_d. It was noticed in [18] that $DL_{n_d}(1, 2d + 1)$ was a first-kind Frobenius circulant. In [11, Theorem 1] it was proved that $b(DL_{n_d}(1, 2d+1)) = d+2$. By using a similar methodology we obtain the following result which generalises [11, Theorem 1] to all 4-valent first-kind Frobenius circulants.

Theorem 4 *Let $n \geq 5$ be an integer all of whose prime factors are congruent to 1 modulo 4. Let h be a solution to (1) and d the diameter of $DL_n(1, h)$ (as given in Lemmas 2 and 3). Then*

$$b(DL_n(1, h)) = d + 2.$$

Moreover, we can explicitly give an optimal broadcasting in $DL_n(1, h)$.

Proof: Denote $G = DL_n(1, h)$. Since G is vertex-transitive, $b(G) = b(G, [u])$ for all $[u] \in \mathbb{Z}_n$. Without loss of generality we may assume that $[0]$ has a message to be broadcasted in G. In the following we prove $b(G, [0]) = d + 2$ and so establish $b(G) = d + 2$.

Part 1: Initially, the message is at $[0]$. A broadcasting is defined by specifying a pair

$$L([u]) = (t_u, [v_u]) \tag{6}$$

for each $[u] \neq [0]$, which means that $[u]$ receives the message at time t_u from a neighbour $[v_u]$ of $[u]$. We require $t_v < t_u$ for $[v] = [v_u]$ since $[v]$ should receive the message before retransmitting it to $[u]$. We also require $(t_u, [v_u]) \neq (t_w, [v_w])$ whenever $[u] \neq [w]$ since no vertex is allowed to send the message to two of its neighbours at the same time.

Let r be as in (4). We successively send the message to the vertices in the negative x-direction at times $1, 2, \ldots, r$, in the x-direction at times $2, 3, \ldots, r + 1$, in the y-direction at times $3, 4, \ldots, r + 2$, and in

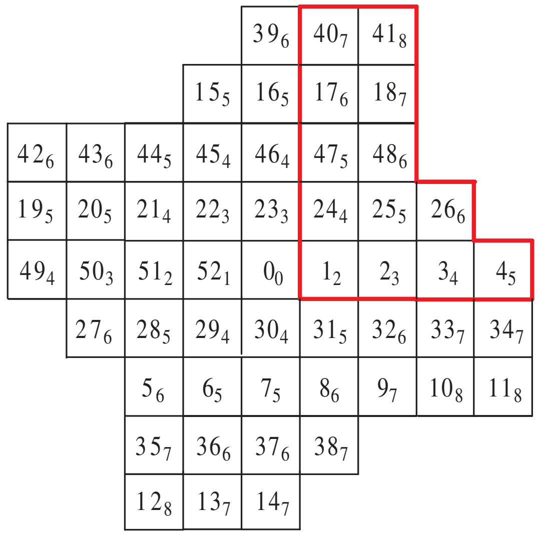

Fig. 2: An optimal broadcasting in $DL_{53}(1, 23)$. Subscripts represent the times that the corresponding vertices receive the message originated from [0]. The part in the first quadrant bounded by bold lines is A.

the negative y-direction at times $4, 5, \ldots, r+2, r+3$, where $r+3$ occurs only when $r < d$. (By Lemma 2 (b), $r = d$ occurs only when $x_r = 0$.) At any time, a vertex $[v]$ that received the message already retransmits the message to the unique up-neighbour $[v+h]$ (first priority) or the unique down-neighbour $[v-h]$ (second priority); if both neighbours have received the message already, then $[v]$ does not send the message to any vertex at that time. In order to fulfill the broadcasting in $d+2$ time steps, we have to take care of those vertices in $-A[h]$ whose distance to [0] is equal to d.

For $0 \le j \le r$, define

$$y_j = \max\{k : 1 \le k \le r, x_k \ge j\}.$$

Let $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. Define

$$L([-j]) = (j, [-(j-1)]),\ L([j]) = (j+1, [j-1]),\ 1 \le j \le r \tag{7}$$

$$L([kh]) = (k+2, [(k-1)h]),\ 1 \le k \le r \tag{8}$$

$$L([-kh]) = (k+3, [-(k-1)h]),\ 1 \le k \le \min\{r, d-1\} \tag{9}$$

$$L([j+kh]) = (j+k+2-\delta_{jr}, [j+(k-1)h]), 1 \le j \le r, 1 \le k \le y_j \tag{10}$$

$$L([-k+jh]) = (j+k+1-\delta_{kr}, [-k+(j-1)h]), 1 \le k \le r, 1 \le j \le x_k \tag{11}$$

$$L([-j-kh]) = (j+k+2-\delta_{jr}, [-j-(k-1)h]), 1 \le j \le r, 1 \le k \le y_j \tag{12}$$

$$L([k-jh]) = (j+k+3-\delta_{kr}, [k-(j-1)h]), 1 \le k \le r, 1 \le j \le x_k, j+k < d. \quad (13)$$

In this way we define a broadcasting on all vertices of G other than those $[k-jh] \in -A[h]$ (that is, $0 \le k \le r, 1 \le j \le x_k$) in the fourth quadrant such that $d([0],[k-jh]) = j+k = d$.

Consider the remaining vertices above. Such a vertex $[k-jh]$ must satisfy $j = x_k$ (for otherwise $d([0],[k-(j+1)h]) = j+k+1 = d+1$ by Lemma 2 (a), which is a contradiction) and hence is of the form $[k-x_kh]$, where $x_k + k = d$ and $x_k \ge 1$. By Lemma 2 (b) and (5), if $a < r$, then $d = x_r + r = 2r - a \ge r+1$, and $[r - x_rh]$ is the only element of $-A[h]$ whose distance to $[0]$ is d and hence is the only exceptional vertex to be considered. In this case, if $x_r = 1$, then since $[r]$ receives the message at time $r+1 = d$, we may define $L([r-x_rh]) = (d+1,[r])$; if $x_r \ge 2$, then since $L([r-(x_r-1)h]) = (d+1,[r-(x_r-2)h])$ by (13), we may define $L([r-x_rh]) = (d+2,[r-(x_r-1)h])$. Thus, if $a < r$, then $[r-x_rh]$ with $x_r + r = d$ receives the message at time $d+1$ or $d+2$. This together with (7)-(13) gives a broadcasting in G using $d+2$ time steps. See Figure 2 for this broadcasting in $DL_{53}(1,23)$.

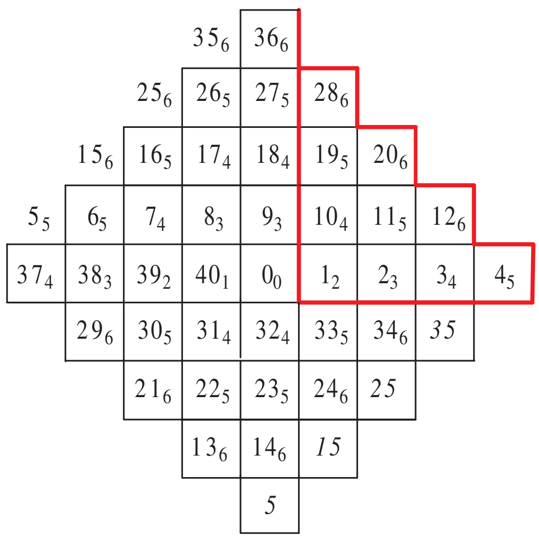

Fig. 3: An optimal broadcasting in $DL_{41}(1,9)$. Subscripts represent the times that the corresponding vertices receive the message originated from $[0]$. The part bounded by bold lines is A, and the other three parts of the minimum distance diagram are obtained by rotating A about the origin by $90^\circ, 180^\circ, 270^\circ$ respectively. $DL_{41}(1,9)$ is the largest connected 4-valent circulant graph with diameter $d = 4$. We have $a = b-1 = r = d = x_0 = 4, x_1 = 3, x_2 = 2, x_3 = 1, x_4 = 0$ and $n = 41 = 5^2 + 4^2$. Notice that $[5],[15],[25],[35]$ receive the message from $[37],[6],[16],[26]$ at times $5,6,6,6$ respectively.

It remains to deal with the case $a = r$. In this case, $x_i = r - i$ for $0 \le i \le r$ by (5), $d = r$ by Lemma 2 (b), and so $[k-x_kh] = [k-(d-k)h]$ is an exceptional vertex for each $k = 0,1,\ldots,d$. Moreover, since $a = r = (a+b-1)/2$, we have $b = a+1 = d+1$, $n = a^2+b^2 = 2d^2+2d+1$ and so $G = DL_{n_d}(1,2d+1)$ by the discussion after Theorem 4. Thus, $h = 2d+1$ and $[(d+1)h] = [d]$.

This implies $[k - x_k h] = [k - (d-k)h] = [-(d-k) + kh + h]$ and hence $[k - x_k h]$ is adjacent to $[-(d-k) + kh]$. However, by (11), $[-(d-k) + kh]$ received the message at time $d + 1 - \delta_{d-k,d}$ for $0 \le k \le d-1$. Thus, we may define $L([k - x_k h]) = (d + 2 - \delta_{d-k,d}, [-(d-k) + kh])$ for $0 \le k \le d-1$. Note that $[d - x_d h] = [d]$ received the message at time $d+1$ (see (7)). So we have finished defining a broadcasting in G using $d+2$ time steps when $a = r$. See Figure 3 for an illustration of this broadcasting.

In summary, we have proved $b(G, [0]) \le d + 2$ up to now.

Part 2: We now prove that $d+2$ is a lower bound for $b(G, [0])$. This is true when $d = 1$ since in this case G is the complete graph $K_5 = DL_5(1, 2)$. Assume $d \ge 2$ in the following. Since the minimum distance diagram is symmetric, each of $A, A[h], -A, -A[h]$ contains at least one vertex whose distance to $[0]$ is d. Let $[u] \in A$ be at distance d from $[0]$. Then $[uh] \in A[h], [-u] \in -A, [-uh] \in -A[h]$ all have distance d to $[0]$. Suppose to the contrary that there exists a broadcasting using $d+1$ time steps. One of the neighbours $[1], [h], [-1], [-h]$ of $[0]$ should receive the message at time 1, and assume that the other three neighbours receive the message at times $t_1 < t_2 < t_3$ respectively, where $t_1 \ge 2$. Note that $[uh^0] = [u], [uh^1] = [uh], [uh^2] = [-u], [uh^3] = [-uh]$ by (1). Let $P_i : [0], [v_i], [w_i], \ldots, [uh^i]$ be the path of G along which the message is sent from $[0]$ to $[uh^i]$, where $[v_i] \in \{[1], [h], [-1], [-h]\}$, $i = 0, 1, 2, 3$. Since $d([0], [uh^i]) = d$, each P_i has length at least d. We may have $[v_i] = [v_j]$ for distinct i and j. Since $t_2 \ge 3, t_3 \ge 4$, if $[v_i]$ receives the message at time t_2 or t_3, then the last vertex $[uh^i]$ of P_i receives the message at time $d+2$ or later, which is a contradiction. Similarly, if $t_1 \ge 3$, then no $[v_i]$ receives the message at time t_1. Hence each $[v_i]$ receives the message at time 1 or $t_1 = 2$. If, for $i \ne j$, both $[v_i]$ and $[v_j]$ receive the message at time 2, then $[v_i] = [v_j]$ and one of $[uh^i]$ and $[uh^j]$ receives the message at time $d+2$ or later, a contradiction. Hence at most one of $[v_0], [v_1], [v_2], [v_3]$ receives the message at time 2 and the remaining three or four vertices receive the message at time 1. Suppose without loss of generality that $[v_0], [v_1], [v_2]$ receive the message at time 1. Then $[v_0] = [v_1] = [v_2]$ and one of $[u], [uh], [-u]$ receives the message at time $d+3$ or later. This final contradiction proves that $b(G, [0])$ is at least $d+2$.

Combining Parts 1 and 2, we obtain $b(G, [0]) = d+2$ and so $b(G) = d+2$. Hence the broadcasting given in Part 1 is optimal for source vertex $[0]$.

An optimal broadcasting for any source vertex $[w]$ can be obtained from the optimal broadcasting L in Part 1 for source vertex $[0]$ by translation. Define

$$L^w([u + w]) = (t_u, [v_u + w])$$

for each $[u] \in \mathbb{Z}_n$, where $(t_u, [v_u])$ is as in (6); that is, the time when the message originated from $[w]$ is sent from $[v_u + w]$ to $[u + w]$ is the same as the time when the message originated from $[0]$ is sent from $[v_u]$ to $[u]$ under L. Since $[x] \mapsto [x + w]$, $[x] \in \mathbb{Z}_n$, is an automorphism of G, L^w above defines a broadcasting for source vertex $[w]$, and it is optimal since $b(G, [w]) = b(G, [0]) = d+2$. $\square$

In the special case of $DL_{n_d}(1, 2d+1)$ the broadcasting described in Part 1 of the proof above is similar to the one given in [11]. Nevertheless, this is by no means the only optimal broadcasting in $DL_{n_d}(1, 2d+1)$. In general, optimal broadcastings of $DL_n(1, h)$ other than the one given in the proof of Theorem 4 can be found by using similar approaches.

4 Recursive construction

An important issue in network design is whether it is possible to 'expand' an existing network to larger ones of similar structures. And if this is possible, how can we construct efficiently such larger networks from smaller ones? For instance, an attractive feature of hypercubes is that we can easily expand a given hypercube to larger ones of higher dimensions. In this section we prove that 4-valent Frobenius circulants share this property. We will give algorithms for constructing larger 4-valent Frobenius circulants from smaller ones by using number theory. To this end we will use an equivalent definition of a 4-valent Frobenius circulant in terms of Gaussian integers.

A *Gaussian integer* is a complex number $a + bi$ with both a and b in $\mathbb{Z}$. (In this section we reserve i for the imaginary unit of complex numbers.) The set $\mathbb{Z}[i]$ of all Gaussian integers is a ring under the usual addition and multiplication of complex numbers, the *ring of Gaussian integers*. Its units are $1, -1, i$ and $-i$, and for $\alpha \in \mathbb{Z}[i]$ and a unit ε we call $\varepsilon\alpha$ an *associate* of α. It is well known that $\mathbb{Z}[i]$ is an Euclidean domain with the norm function defined by $N(a + bi) = a^2 + b^2$ for $0 \neq a + bi \in \mathbb{Z}[i]$. In other words, for any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \gamma\beta + \delta$ and either $\delta = 0$ or $N(\delta) < N(\beta)$. Hence $\mathbb{Z}[i]$ is a principal ideal domain and so a unique factorization domain. It is easy to see that $N(\alpha\beta) = N(\alpha)N(\beta)$ for any nonzero $\alpha, \beta \in \mathbb{Z}[i]$. All these results and definitions about Gaussian integers can be found in, for example, [10].

Given $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, let $\mathbb{Z}[i]_\alpha = \mathbb{Z}[i]/(\alpha)$ denote the quotient ring of $\mathbb{Z}[i]$ with respect to the principal ideal (α) of $\mathbb{Z}[i]$. Denote by $[\beta]_\alpha = \beta + (\alpha)$ the residue class modulo α containing β. For $\beta, \gamma \in \mathbb{Z}[i]$, define [12] $d_\alpha([\beta]_\alpha, [\gamma]_\alpha)$ to be the minimum value of $|x|+|y|$ such that $[\beta-\gamma]_\alpha = [x+yi]_\alpha$. Then d_α is a metric in $\mathbb{Z}[i]_\alpha$ [12, Theorem 2]. In the case when $\gcd(a, b) = 1$, the *Gaussian graph* G_α generated by α is defined [12] to have vertex set $\mathbb{Z}[i]_\alpha$ such that $[\beta]_\alpha, [\gamma]_\alpha$ are adjacent if and only if $d_\alpha([\beta]_\alpha, [\gamma]_\alpha) = 1$. In other words, G_α is the Cayley graph $\mathrm{Cay}(\mathbb{Z}[i]_\alpha, H_\alpha)$ on the additive group of $\mathbb{Z}[i]_\alpha$, where

$$H_\alpha = \{[1]_\alpha, -[1]_\alpha, [i]_\alpha, -[i]_\alpha\}. \tag{14}$$

Note that, if α is an associate of $1 + i$ (that is, $N(\alpha) = 2$), then the cardinality of H_α is 2 and so G_α is 2-valent. In general, G_α is a 4-valent graph as long as $\gcd(a, b) = 1$ and α is not an associate of $1 + i$. One can verify that $G_\alpha \cong G_{\varepsilon\alpha}$ for any unit ε of $\mathbb{Z}[i]$, and $\mathbb{Z}[i]_\alpha \to \mathbb{Z}[i]_{\varepsilon\alpha}, [\beta]_\alpha \mapsto [\varepsilon\beta]_{\varepsilon\alpha}$ defines an isomorphism between the two graphs. Since $\varepsilon\alpha = a + bi, -a - bi, -b + ai, b - ai$ when ε runs over the four units of $\mathbb{Z}[i]$, in studying Gaussian graphs we may assume without loss of generality that both a and b are positive integers.

Gaussian graphs above were introduced in [12] with motivation from coding theory. It turns out that in the case when $N(\alpha) = a^2 + b^2$ is odd, they are exactly the family of 4-valent Frobenius circulants. This was first noticed by Alison Thomson (personal communication). It is implied in the following lemma in which $N(\alpha)$ can be odd or even.

Lemma 5

(a) Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ be such that $a, b > 0$, $\gcd(a, b) = 1$ and $N(\alpha) > 2$. Then $G_\alpha \cong DL_{N(\alpha)}(1, l)$, where l is the unique solution to $x^2 + 1 \equiv 0 \pmod{N(\alpha)}$ such that $al \equiv b \pmod{N(\alpha)}$.

(b) Conversely, for any solution l to $x^2 + 1 \equiv 0 \pmod{n}$, we have $DL_n(1, l) \cong G_\alpha$, where $\alpha = a + bi$ with $a, b > 0$ the unique nonnegative primitive solution to $x^2 + y^2 = n$ such that $al \equiv b \pmod{n}$.

Proof:

(a) Since $a^2 + b^2 = N(\alpha)$ and $\gcd(a, b) = 1$, by [15, Theorem 6.4], there exists a unique solution l to $x^2 + 1 \equiv 0 \pmod{N(\alpha)}$ such that $al \equiv b \pmod{N(\alpha)}$. Define

$$\phi : \mathbb{Z}_{N(\alpha)} \to \mathbb{Z}[i]_\alpha,\ [x + yl] \mapsto [x + yi]_\alpha, \tag{15}$$

where $[x + yl]$ is the residue class of $x + yl$ modulo $N(\alpha)$.

We claim that ϕ is a well-defined mapping. In fact, if $x+y \equiv x'+y'l \pmod{N(\alpha)}$, then $a(x-x')+b(y-y') \equiv 0 \pmod{N(\alpha)}$ since $al \equiv b \pmod{N(\alpha)}$. Thus $a(x-x')+b(y-y') = s(a^2+b^2)$ for some $s \in \mathbb{Z}$. The only solutions to this Diophantine equation are $x-x' = sa+bt, y-y' = sb-at$ for $t \in \mathbb{Z}$. Hence $(x - x') + (y - y')i = (s - ti)\alpha$ and so $[x + yi]_\alpha = [x' + y'i]_\alpha$.

It is clear that ϕ is surjective. Suppose $[x + yi]_\alpha = [x' + y'i]_\alpha$. Then $(x - x') + (y - y')i = (c + di)(a + bi)$ for some $c + di \in \mathbb{Z}[i]$; that is, $x - x' = ac - bd$ and $y - y' = ad + bc$. Hence $a(x - x') + b(y - y') \equiv 0 \pmod{N(\alpha)}$. Since $\gcd(a, b) = 1$, we have $\gcd(a, N(\alpha)) = 1$ and so $aa' \equiv 1 \pmod{N(\alpha)}$ for some $a' \in \mathbb{Z}$. Using $al \equiv b \pmod{N(\alpha)}$, we then have $aa'(x - x') + aa'l(y - y') \equiv 0 \pmod{N(\alpha)}$ and so $x + yl \equiv x' + y'l \pmod{N(\alpha)}$. Therefore, ϕ is injective and hence bijective. Since $\phi([1]) = [1]_\alpha$ and $\phi([l]) = [i]_\alpha$, one can see that ϕ is an isomorphism from $DL_{N(\alpha)}(1, l)$ to G_α.

(b) Given a solution l to $x^2 + 1 \equiv 0 \pmod{n}$, by [15, Theorem 6.5] there is a unique primitive solution $a, b > 0$ to $x^2 + y^2 = n$ such that $al \equiv b \pmod{n}$. Similar to the proof above, one can verify $DL_n(1, l) \cong G_\alpha$, where $\alpha = a + bi$. □

Remark 6

(i) In part Lemma 5 (a), there exists a unique solution l' to $x^2 + 1 \equiv 0 \pmod{N(\alpha)}$ such that $bl' \equiv a \pmod{N(\alpha)}$. Since $\gcd(a, N(\alpha)) = \gcd(b, N(\alpha)) = 1$, from $al \equiv b$, $bl' \equiv a \pmod{N(\alpha)}$ we have $ll' \equiv 1 \pmod{N(\alpha)}$. Since $l^4 \equiv 1 \pmod{N(\alpha)}$, it follows that $l' \equiv l^3 \equiv -l \pmod{N(\alpha)}$ and so $DL_n(1, l) = DL_n(1, l')$. Thus we may assume $0 < a < b$ in (a) without loss of generality. Similarly, we may assume $0 < a < b$ in Lemma 5 (b).

(ii) It is known that the Diophantine equation $x^2 + y^2 = n$ has a nonnegative primitive solution if and only if every odd prime factor of n is congruent to 1 modulo 4 (see e.g. [15, Corollary 6.8.2 and pp.320]). In the case when $N(\alpha)$ is odd in (a) and n is odd in (b) of Lemma 5, $DL_{N(\alpha)}(1, l)$ is a 4-valent first-kind Frobenius graph. Hence the family of 4-valent first-kind Frobenius circulants is identical to the family of Gaussian graphs of odd orders.

(iii) That n is even can occur, but in this case the corresponding $DL_n(1, l)$ is not a first-kind Frobenius circulant because the subgroup $\{[1], [l], -[1], -[l]\}$ of $\mathbb{Z}_n^*$ is not regular on $\mathbb{Z}_n \setminus \{[0]\}$. For example, $(3, 5)$ is a primitive solution to $x^2 + y^2 = 34$ and the corresponding l is 13 as $3 \cdot 13 \equiv 5 \pmod{34}$ and $13^2 + 1 \equiv 0 \pmod{34}$. However, since $[12], -[2]$ and $-[14]$ are not in $\mathbb{Z}_{34}^*$, by [18, Lemma 4], $\{[1], [13], -[1], -[13]\}$ is not regular on $\mathbb{Z}_{34} \setminus \{[0]\}$ and so $DL_{34}(1, 13)$ is not a Frobenius graph.

The set H_α defined in (14) is a subgroup of the group $\mathbb{Z}[i]_\alpha^*$ of units of ring $\mathbb{Z}[i]_\alpha$. One can verify that $(x+yi)^{i^s} = (x+yi)i^s$ defines an action (as a group) of H_α on the additive group of $\mathbb{Z}[i]_\alpha$, where $x+yi, i^s$

and $(x+yi)i^s$ are interpreted as their residue classes modulo α. Hence $\mathbb{Z}[i]_\alpha \rtimes H_\alpha$ is well-defined and moreover it acts on $\mathbb{Z}[i]_\alpha$ (as a set) by

$$(x+yi)^{(c+di,i^s)} = ((x+c)+(y+d)i)i^s,\ x+yi \in \mathbb{Z}[i]_\alpha,\ (c+di,i^s) \in \mathbb{Z}[i]_\alpha \rtimes H_\alpha,$$

where the Gaussian integers involved are interpreted as their residue classes modulo α. One can verify that $\mathbb{Z}[i]_\alpha \rtimes H_\alpha$ preserves adjacency and non-adjacency of G_α. So it can be regarded as a group of automorphisms of G_α. Moreover, by [21, Lemma 2.1] and the fact that the group H_α is transitive on the connection set H_α of G_α, we have

Lemma 7 *Every Gaussian graph G_α is $\mathbb{Z}[i]_\alpha \rtimes H_\alpha$-arc-transitive.*

When $N(\alpha)$ is odd this is known in [18] in view of Lemmas 1 and 5. In this case one can prove that $\mathbb{Z}[i]_\alpha \rtimes H_\alpha$ is a Frobenius group.

To construct larger 4-valent Frobenius circulants from smaller ones, by Lemma 5 it suffices to find an approach to constructing larger Gaussian graphs of odd order from smaller ones. The following lemma serves for this purpose, and it applies to a broader family of graphs. Note that for any $0 \neq \alpha = a+bi \in \mathbb{Z}[i]$ we can define $G_\alpha = \mathrm{Cay}(\mathbb{Z}[i]_\alpha, H_\alpha)$ as before without requiring $\gcd(a,b)=1$, where H_α is as in (14). To ensure G_α is a nontrivial graph with valency 4, we require that α is not a unit or an associate of 2 or $1+i$, or equivalently $N(\alpha) \geq 5$. Such generalized Gaussian graphs were studied in [13] (but with the necessary condition $N(\alpha) \geq 5$ neglected).

A graph G_1 is called a *cover* of a graph G_2 if there exists a surjective mapping $\phi : V(G_1) \to V(G_2)$ such that for each $u \in V(G_1)$, the restriction of ϕ to the neighbourhood $N_{G_1}(u)$ of u in G_1 is a bijection from $N_{G_1}(u)$ to the neighbourhood $N_{G_2}(\phi(u))$ of $\phi(u)$ in G_2. We say that G_1 is a *k-fold cover* of G_2 if in addition $k = |\phi^{-1}(v)|$ for all $v \in V(G_2)$.

Lemma 8 *Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $N(\alpha), N(\beta) \geq 5$. Then $G_{\alpha\beta}$ can be constructed from G_α and is an $N(\beta)$-fold cover of G_α.*

Proof: Let $K = ([\alpha]_{\alpha\beta})$ be the principal ideal of $\mathbb{Z}[i]_{\alpha\beta}$ induced by $[\alpha]_{\alpha\beta}$. Since $\mathbb{Z}[i]$ is Euclidean, its elements are of the form $\xi = \eta\beta + \delta$ with $\delta = 0$ or $N(\delta) < N(\beta)$. Hence $K = \{[\alpha\delta]_{\alpha\beta} : \delta \in \mathbb{Z}[i],\ \delta = 0 \text{ or } N(\delta) < N(\beta)\}$. Since $K = (\alpha)/(\alpha\beta)$, when it is viewed as a subgroup of the additive group of $\mathbb{Z}[i]_{\alpha\beta}$, we have $\mathbb{Z}[i]_\alpha \cong \mathbb{Z}[i]_{\alpha\beta}/K$ via the classical isomorphism $[\xi]_\alpha \mapsto K + [\xi]_{\alpha\beta},\ [\xi]_\alpha \in \mathbb{Z}[i]_\alpha$. Hence $|K| = N(\alpha\beta)/N(\alpha) = N(\beta)$.

Now we construct $G_{\alpha\beta}$ from G_α as follows. Consider an arbitrary pair of adjacent vertices $[\xi]_\alpha, [\xi']_\alpha$ of G_α. By the definition of G_α, there exist $\eta \in \mathbb{Z}[i]$ and a unit ε of $\mathbb{Z}[i]$, both relying on ξ and ξ', such that $\xi - \xi' = \alpha\eta + \varepsilon$. Construct a graph $\hat{G}_{\alpha\beta}$ with vertex set $\mathbb{Z}[i]_{\alpha\beta}$ such that

$$\begin{aligned}\text{each } [\alpha\delta+\xi]_{\alpha\beta} \in K + [\xi]_{\alpha\beta} \text{ is adjacent to } [\alpha\delta+\xi-\varepsilon]_{\alpha\beta} = [\alpha(\delta+\eta)+\xi']_{\alpha\beta} \in K + [\xi']_{\alpha\beta} \\ \text{and } [\alpha\delta+\xi]_{\alpha\beta} \text{ is not adjacent to any other element in } K + [\xi']_{\alpha\beta}. \quad (16)\end{aligned}$$

Note that this adjacency relation is defined for all pairs of adjacent vertices $[\xi]_\alpha, [\xi']_\alpha$ of G_α. Since $\xi' - \xi = -\alpha\eta - \varepsilon$, when interchanging the roles of $[\xi]_\alpha$ and $[\xi']_\alpha$ in (16), we obtain that $[\alpha\delta+\xi-\varepsilon]_{\alpha\beta} = [\alpha(\delta+\eta)+\xi']_{\alpha\beta}$ is adjacent to $[\alpha(\delta+\eta)+\xi'+\varepsilon]_{\alpha\beta} = [\alpha\delta+\xi]_{\alpha\beta}$ in $\hat{G}_{\alpha\beta}$. Hence the adjacency relation (16) is symmetric. Moreover, it is independent of the choice of representatives of $[\xi]_\alpha$ and $[\alpha\delta+\xi]_{\alpha\beta}$. In fact, if $[\alpha\delta_1+\xi_1]_{\alpha\beta} = [\alpha\delta+\xi]_{\alpha\beta}$ (which implies $[\xi_1]_\alpha = [\xi]_\alpha$), then $\xi_1 = \xi + \alpha(\sigma\beta+\delta-\delta_1)$ for some

$\sigma \in \mathbb{Z}[i]$ and hence $\xi_1 - \xi' = \alpha(\sigma\beta + \delta - \delta_1 + \eta) + \varepsilon$. Thus, by (16), $[\alpha\delta_1 + \xi_1]_{\alpha\beta} \in K + [\xi]_{\alpha\beta}$ is adjacent to $[\alpha(\delta_1 + (\sigma\beta + \delta - \delta_1 + \eta)) + \xi']_{\alpha\beta} = [\alpha(\delta + \eta) + \xi']_{\alpha\beta} \in K + [\xi']_{\alpha\beta}$, which agrees with (16) applied to $[\alpha\delta + \xi]_{\alpha\beta}$. Therefore, $\hat{G}_{\alpha\beta}$ is well-defined as an undirected graph. Since G_α is 4-valent, by its definition $\hat{G}_{\alpha\beta}$ is 4-valent as well. We now prove that it is exactly the generalized Gaussian graph $G_{\alpha\beta}$.

Using the notation above, obviously $[\alpha\delta + \xi]_{\alpha\beta}$ and $[\alpha\delta + \xi - \varepsilon]_{\alpha\beta}$ are adjacent in $G_{\alpha\beta}$. Thus, by (16), if two vertices are adjacent in $\hat{G}_{\alpha\beta}$, then they are adjacent in $G_{\alpha\beta}$. Conversely, suppose $[\zeta]_{\alpha\beta}$ and $[\zeta']_{\alpha\beta}$ are adjacent in $G_{\alpha\beta}$. Then $\zeta - \zeta' = \tau(\alpha\beta) + \varepsilon$ for some $\tau \in \mathbb{Z}[i]$ and a unit ε of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is Euclidean, we can write $\zeta = \alpha\delta + \xi$ and $\zeta' = \alpha\delta' + \xi'$, where $\xi = 0$ or $N(\xi) < N(\alpha)$, and $\xi' = 0$ or $N(\xi') < N(\alpha)$. Thus $[\alpha\delta + \xi]_{\alpha\beta} = [\alpha\delta' + \xi']_{\alpha\beta} + [\varepsilon]_{\alpha\beta}$. Since $[\zeta]_{\alpha\beta} = [\alpha\delta + \xi]_{\alpha\beta}$ and $[\zeta']_{\alpha\beta} = [\alpha\delta' + \xi']_{\alpha\beta} = [\alpha\delta + \xi - \varepsilon]_{\alpha\beta}$, by the definition of $\hat{G}_{\alpha\beta}$, $[\zeta]_{\alpha\beta}$ and $[\zeta']_{\alpha\beta}$ are adjacent in $\hat{G}_{\alpha\beta}$. Therefore, $G_{\alpha\beta}$ is identical to $\hat{G}_{\alpha\beta}$ and so can be constructed from G_α as in the previous paragraph. It is obvious that the quotient graph of $G_{\alpha\beta}$ with respect to the partition $\mathbb{Z}[i]_{\alpha\beta}/K$ of $\mathbb{Z}[i]_{\alpha\beta}$ is isomorphic to G_α, and moreover $G_{\alpha\beta}$ is an $N(\beta)$-fold cover of G_α. $\square$

We now give procedures for constructing larger 4-valent first-kind Frobenius circulants from smaller ones. The case below for prime power orders is a straightforward application of relevant results in number theory. (The uniqueness of $DL_{p^e}(1, h(e))$ follows from [18, Theorem 2].)

Procedure 9

Input: A prime $p \equiv 1 \pmod 4$.

Output: The unique 4-valent first-kind Frobenius circulant $DL_{p^e}(1, h(e))$ of order p^e, for every integer $e \geq 1$, where $h(e)$ is a solution to $x^2 + 1 \equiv 0 \pmod{p^e}$.

1. By the well-known Lagrange Theorem, $h(1) \equiv ((p-1)/2)! \pmod p$; this gives $DL_p(1, h(1))$;

2. suppose $DL_{p^e}(1, h(e))$ has been constructed for some $e \geq 1$, we construct $DL_{p^{e+1}}(1, h(e+1))$ by using $h(e+1) = h(e) + p^e w$ (see e.g. [14, Section 2.6]), where w is a solution to the congruence equation $2h(e)x \equiv -(h(e)^2 + 1)/p^e \pmod p$.

The graphs

$$DL_p(1, h(1)), DL_{p^2}(1, h(2)), \ldots, DL_{p^e}(1, h(e)), DL_{p^{e+1}}(1, h(e+1)), \ldots \tag{17}$$

thus constructed are both interesting and important because they are building blocks for constructing all 4-valent first-kind Frobenius circulants as we will see below. By Lemma 8 each graph in this sequence is a cover of the graphs preceding it. We notice that the ‘smallest’ graph $DL_p(1, h(1))$ in the sequence is exactly $C(p; \pm 1, \pm h(1))$ in [5, Theorem 1.2(c)], which plays a significant role in the classification [5, Theorem 1.2] of a family of arc-transitive graphs.

The following procedure deals with the case of composite integers.

Procedure 10

Input: A 4-valent first-kind Frobenius circulant $DL_n(1, h)$, defined by an integer $n \geq 5$ with all prime factors congruent to 1 modulo 4 and a solution h to (1); a prime $p \equiv 1 \pmod 4$ which is not a divisor of n; and an integer $e \geq 1$.

Output: Two non-isomorphic 4-valent first-kind Frobenius circulants of order np^e obtained by expanding $DL_n(1, h)$.

1. Find the unique nonnegative primitive solution (a, b) to (3) such that $ah \equiv b \pmod n$, and set $\alpha = a + bi$;
2. find a nonnegative primitive solution (c, d) to $x^2 + y^2 = p^e$, and set $\beta = c + di$;
3. construct $G_{\alpha\beta}$ and $G_{\alpha\bar{\beta}}$ based on G_α by using rule (16);
4. let ε_1 be the unique unit of $\mathbb{Z}[i]$ such that $\varepsilon_1\alpha\beta = a_1 + b_1 i$ satisfies $a_1, b_1 > 0$, and ε_2 the unique unit of $\mathbb{Z}[i]$ such that $\varepsilon_2\alpha\bar{\beta} = a_2 + b_2 i$ satisfies $a_2, b_2 > 0$; find the unique solution h_j to $x^2 + 1 \equiv 0 \pmod{np^e}$ such that $a_j h_j \equiv b_j \pmod{np^e}$, $j = 1, 2$;
5. construct $DL_{np^e}(1, h_1)$ and $DL_{np^e}(1, h_2)$.

Remark 11 We may use standard algorithms in number theory to find (a, b) in Step 1 and h_j in Step 4. See for example the proofs of [15, Theorems 6.4 and 6.5]. We may obtain (c, d) in Step 2 by recursively computing $h(e)$ in Procedure 9 and then applying the algorithm implied in the proof of [15, Theorem 6.5].

Theorem 12 *Procedure 10 is correct, that is,* $DL_{np^e}(1, h_1)$ *and* $DL_{np^e}(1, h_2)$ *above are 4-valent first-kind Frobenius circulants, and moreover* $DL_{np^e}(1, h_1) \ncong DL_{np^e}(1, h_2)$.

Proof: Using the notation above, we have $DL_n(1, h) \cong G_\alpha$ by Lemma 5. Since $p \equiv 1 \pmod 4$, the Diophantine equation $x^2 + y^2 = p^e$ has exactly two nonnegative primitive solutions. (This can be deduced from, say, [15, Corollaries 6.5.1 and 6.8.1].) Thus (c, d) in Step 2 exists and the other nonnegative primitive solution is (d, c).

Note that $\alpha\beta = (ac - bd) + (ad + bc)i$ gives rise to the solution $(ac - bd, ad + bc)$ to $x^2 + y^2 = np^e$. We claim that this is a primitive solution. Suppose otherwise. Then there exists a prime q in $\mathbb{Z}$ which divides both $ac - bd$ and $ad + bc$. If q divides a, then it divides both bd and bc. Since q cannot divide b due to $\gcd(a, b) = 1$, it follows that q divides both c and d, which contradicts the assumption $\gcd(c, d) = 1$. So q is not a divisor of a. Similarly, q is not a divisor of b, c or d. Since q divides $ac - bd$ and $ad + bc$, it divides $c(ac-bd)+d(ad+bc) = a(c^2+d^2) = ap^e$ and $a(ac-bd)+b(ad+bc) = c(a^2+b^2) = cn$. Since q divides neither a nor c, it follows that q divides p^e and n, and hence $q = p$ is a prime factor of n, which contradicts our assumption. Therefore, $(ac-bd, ad+bc)$ is a primitive solution to $x^2+y^2 = np^e$. It is clear that there is a unique unit ε_1 of $\mathbb{Z}[i]$ such that $\varepsilon_1\alpha\beta = a_1 + b_1 i$ satisfies $a_1, b_1 > 0$. Then (a_1, b_1) is a nonnegative primitive solution to $x^2 + y^2 = np^e$. Moreover, $G_{\varepsilon_1\alpha\beta} \cong G_{\alpha\beta}$ and so $G_{\varepsilon_1\alpha\beta}$ is constructed from G_α via $G_{\alpha\beta}$. (See the discussion following (14).) From Lemma 5 (a) it follows that $DL_{np^e}(1, h_1)$ with h_1 defined in Step 4 is a 4-valent first-kind Frobenius circulant. Similarly, $\alpha\bar{\beta} = (ac + bd) + (-ad + bc)i$ gives rise to a primitive solution $(ac - bd, ad + bc)$ to $x^2 + y^2 = np^e$, and hence $DL_{np^e}(1, h_2)$ with h_2 given in Step 4 is a 4-valent first-kind Frobenius circulant.

To prove $DL_{np^e}(1,h_1) \ncong DL_{np^e}(1,h_2)$, it suffices to prove $G_{\alpha\beta} \ncong G_{\alpha\bar{\beta}}$, or equivalently $DL_{np^e}(ac-bd, ad+bc) \ncong DL_{np^e}(ac+bd, -ad+bc)$ by Lemma 5 and the comments before Lemma 3. Suppose otherwise. Then there exists $k \in \mathbb{Z}$ coprime to np^e such that $\{[ac-bd]_{np^e}, [ad+bc]_{np^e}\} = [k]_{np^e} \cdot \{[ac+bd]_{np^e}, [-ad+bc]_{np^e}\}$, where $[x]_{np^e}$ is the residue class in $\mathbb{Z}$ containing x modulo np^e. If $[ac-bd]_{np^e} = [k(ac+bd)]_{np^e}$ and $[ad+bc]_{np^e} = [k(-ad+bc)]_{np^e}$, then there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha\beta = (\alpha\beta)\overline{(\alpha\beta)}\gamma + k(\alpha\bar{\beta})$, that is, $\beta = (\bar{\alpha}\beta\gamma + k)\bar{\beta}$. Thus $N(\beta) = N(\bar{\alpha}\beta\gamma + k)N(\bar{\beta}) = N(\bar{\alpha}\beta\gamma + k)N(\beta)$. Hence $N(\bar{\alpha}\beta\gamma + k) = 1$ and $\bar{\alpha}\beta\gamma + k$ is a unit of $\mathbb{Z}[i]$. It follows that $\beta = c+di = c-di, -c+di, d+ci$ or $-d-ci$; that is, $d=0$, $c=0$, $c=d$ or $c=-d$, which violates the assumption $\gcd(c,d)=1$. If $[ac-bd]_{np^e} = [k(-ad+bc)]_{np^e}$ and $[ad+bc]_{np^e} = [k(ac+bd)]_{np^e}$, then there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha\beta = (\alpha\beta)\overline{(\alpha\beta)}\gamma + ki(\bar{\alpha}\beta)$, that is, $\alpha = (\alpha\bar{\beta}\gamma + ki)\bar{\alpha}$. Thus $\alpha\bar{\beta}\gamma + ki$ is a unit of $\mathbb{Z}[i]$ and so $b=0$, $a=0$, $a=b$ or $a=-b$, which contradicts $\gcd(a,b)=1$. □

Remark 13 Combining Procedures 9 and 10, we have a well understood mechanism to 'expand' a graph in the family of 4-valent first-kind Frobenius circulants to a larger one in the same family.

Example 14 *In the case when $p=5$, by Procedure 9 we recursively obtain $h(1)=2, h(2)=7, h(3)=57, \ldots$ and $K_5 = DL_5(1,2) \cong G_{1+2i}, DL_{5^2}(1,7) \cong G_{4+3i}$, $DL_{5^3}(1,57) \cong G_{11+2i}, \ldots$ Similarly, for $p=13$ we have $h(1)=5, h(2)=70, h(3)=239, \ldots$ and $DL_{13}(1,5) \cong G_{3+2i}$, $DL_{13^2}(1,70) \cong G_{5+12i}, DL_{13^3}(1,239) \cong G_{9+46i}, \ldots$*

Using Procedure 10 and the computation above, we can construct two 4-valent first-kind Frobenius circulants of order, say, $5^3 \cdot 13^2 = 21125$. We first compute $(11+2i)(5+12i) = 31+142i$ and $(11+2i)(5-12i) = 79-122i$. From the former we obtain $31^2+142^2 = 5^3 \cdot 13^2$ and the unique $h>0$ satisfying $31h \equiv 142$ and $h^2+1 \equiv 0 \pmod{5^3 \cdot 13^2}$ is $h=8182$. Hence $DL_{5^3 \cdot 13^2}(1,8182) \cong G_{31+142i}$ is a first-kind Frobenius circulant. For $79-122i$ we use its associate $i(79-122i) = 122+79i$. We have $122^2+79^2 = 5^3 \cdot 13^2$ and the unique $h>0$ satisfying $122h \equiv 79$ and $h^2+1 \equiv 0 \pmod{5^3 \cdot 13^2}$ is $h=18182$. Hence $DL_{5^3 \cdot 13^2}(1,18182) \cong G_{122+79i}$ ($\ncong DL_{5^3 \cdot 13^2}(1,8182)$) is a first-kind Frobenius circulant. Both $DL_{5^3 \cdot 13^2}(1,8182)$ and $DL_{5^3 \cdot 13^2}(1,18182)$ can be constructed from $DL_{5^3}(1,57)$ or $DL_{13^2}(1,70)$ by using the method in the proof of Lemma 8, and they are 13^2-fold covers of $DL_{5^3}(1,57)$ and 5^3-fold covers of $DL_{13^2}(1,70)$.

5 Concluding remarks

In this paper we proved that 4-valent first-kind Frobenius circulants have the minimum possible broadcasting time, namely their diameter plus two, and we explicitly gave optimal broadcasting in such graphs. We developed an approach to constructing larger 4-valent first-kind Frobenius circulants from smaller ones by using number theory. Our results in this regard can be easily generalised to Gaussian graphs of even order.

As mentioned in the introduction, if $n \geq 5$ has l distinct prime divisors and all of them are congruent to 1 modulo 4, then there are exactly 2^{l-1} pairwise non-isomorphic 4-valent first-kind Frobenius circulants of order n [18, Theorem 2].

Question 15 *What is the minimum diameter among such 2^{l-1} graphs of a given order n?*

As mentioned earlier, there is a one-to-one correspondence between solutions h to $x^2+1 \equiv 0 \bmod n$ and nonnegative primitive solutions (a,b) to $x^2+y^2=n$ with $0<a<b$ and $ah \equiv b \bmod n$. Since

by Lemma 3 the diameter of $DL_n(1,h)$ is equal to $b-1$, the question above is equivalent to the one of finding the smallest $b-1$ among all such solutions (a,b).

For example, when $n = 65 = 5 \cdot 13$, both $h_1 = 8$ and $h_2 = 18$ are solutions to $x^2+1 \equiv 0 \bmod 65$, and the corresponding nonnegative primitive solutions to $x^2+y^2 = 65$ such that $0 < a_j < b_j$ and $a_j h_j \equiv b_j \bmod 65$ are $(a_1, b_1) = (1,8)$ and $(a_2, b_2) = (4,7)$. Since 65 has only two distinct prime divisors, $DL_{65}(1,8)$ and $DL_{65}(1,18)$ are the only non-isomorphic 4-valent first-kind Frobenius circulants of order 65, and the answer to Question 15 is 6 when $n = 65$.

Acknowledgements

The author appreciates the referees for their helpful comments and Alison Thomson for bringing [12, 13] to his attention. He is supported by a Future Fellowship (FT110100629) of the Australian Research Council. Part of the work was done during his visit to Shanghai University where he was supported by a Shanghai Leading Academic Discipline Project (No. S30104).

References

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

[2] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, New York, 1996.

[3] X. G. Fang, C. H. Li and C. E. Praeger, On orbital regular graphs and Frobenius graphs, *Discrete Math.* **182** (1998), 85–99.

[4] X. G. Fang and S. Zhou, Gossiping and routing in second-kind Frobenius graphs, *Europ. J. Combin.* **33** (2012), 1001–1014.

[5] A. Gardiner and C. E. Praeger, On 4-valent symmetric graphs, *Europ. J. Combin.* **15** (1994), 375–381.

[6] M.-C. Heydemann, Cayley graphs and interconnection networks, in: G. Hahn and G. Sabidussi eds., *Graph Symmetry*, Kluwer Academic Publishing, Dordrecht, 1997, pp.167–224.

[7] J. Hromkovič, R. Klasing, B. Monien and R. Peine, Dissemination of information in interconnection networks (broadcasting and gossiping), in: D-Z. Du and D. F. Hsu eds., *Combinatorial Network Theory*, Kluwer Academic Publishers, 1996, pp.125–212.

[8] F. K. Hwang, A complementary survey on double-loop networks, *Theoret. Comput. Sci.* **263** (2001), 211–229.

[9] F. K. Hwang, A survey on multi-loop networks, *Theoret. Comput. Sci.* **299** (2003), 107–121.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition, Springer-Verlag, New York, 1990.

[11] A. L. Liestman, J. Opatrny and M. Zaragozá, Network properties of double and triple fixed step graphs, *Intern. J. Foundations of Com. Sci.* **9** (1998), 57–76.

[12] C. Martínez, R. Beivide and E. M. Gabidulin, Perfect codes for metrics induced by circulant graphs, *IEEE Transactions on Information Theory* **53** (2007), 3042–3052.

[13] C. Martínez, R. Beivide, E. Stafford, M. Moretó and E. M. Gabidulin, Modeling toroidal networks with the Gaussian integers, *IEEE Transactions on Computers* **57** (2008), no. 8, 1046–1056.

[14] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1980.

[15] D. Redmond, *Number Theory*, Marcel Dekker, Inc., New York, Basel, Hong Kong, 1996.

[16] P. Solé, The edge-forwarding index of orbital regular graphs, *Discrete Math.* **130** (1994), 171–176.

[17] A. Thomson, *Frobenius graphs as interconnection networks*, Ph.D. Thesis, The University of Melbourne, 2011.

[18] A. Thomson and S. Zhou, Frobenius circulant graphs of valency four, *J. Austral. Math. Soc.* **85** (2008), 269–282.

[19] C. K. Wong and Don Coppersmith, A combinatorial problem related to multimodule memory organizations, *J. Assoc. Comp. Mach.* **21** (3) (1974), 392–402.

[20] 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.

[21] S. Zhou, A class of arc-transitive Cayley graphs as models for interconnection networks, *SIAM J. Disc. Math.* **23** (2009), 694–714.