Rotational circulant graphs

Alison Thomson and Sanming Zhou

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

September 4, 2013

Abstract

A Frobenius group is a transitive permutation group which is not regular but only the identity element can fix two points. Such a group can be expressed as the semi-direct product \( G = K \rtimes H \) of a nilpotent normal subgroup \( K \) and another group \( H \) fixing a point. A first-kind \( G \)-Frobenius graph is a connected Cayley graph on \( K \) with connection set an \( H \)-orbit \( a^H \) on \( K \) that generates \( K \), where \( H \) has an even order or \( a \) is an involution. It is known that the first-kind Frobenius graphs admit attractive routing and gossiping algorithms. A complete rotation in a Cayley graph on a group \( G \) with connection set \( S \) is an automorphism of \( G \) fixing \( S \) setwise and permuting the elements of \( S \) cyclically. It is known that if the fixed-point set of such a complete rotation is an independent set and not a vertex-cut, then the gossiping time of the Cayley graph (under a certain model) attains the smallest possible value. In this paper we classify all first-kind Frobenius circulant graphs that admit complete rotations, and describe a means to construct them. This result can be stated as a necessary and sufficient condition for a first-kind Frobenius circulant to be 2-cell embeddable on a closed orientable surface as a balanced regular Cayley map. We construct a family of non-Frobenius circulants admitting complete rotations such that the corresponding fixed-point sets are independent and not vertex-cuts. We also give an infinite family of counterexamples to the conjecture that the fixed-point set of every complete rotation of a Cayley graph is not a vertex-cut.

Key words: Circulant graph; Frobenius group; Frobenius graph; gossiping; balanced regular Cayley map; HARTS; hexagonal mesh

AMS Subject Classification (2010): 05C25, 68M10, 68R10

1 Introduction

1.1 Motivation

Given a group \( G \) with identify element \( 1 \) and a subset \( S \) of \( G \) with \( 1 \not\in S \) and \( S = S^{-1} := \{s^{-1} : s \in S\} \), the Cayley graph on \( G \) with connection set \( S \), denoted \( \text{Cay}(G,S) \), is the graph with vertex set \( G \) such that \( g,h \in G \) are adjacent if and only if \( gh^{-1} \in S \). A Cayley graph on a cyclic group is called a circulant graph (or circulant for short), or a multi-loop network as used in computer science.

It is widely recognized \([1, 3, 11, 19]\) that Cayley graphs provide good models for interconnection networks, and as such they have been studied extensively in computer science for more than two decades. In particular, since the 1970s \([37]\), circulant graphs have attracted attention due to their regularity, simple structure and rich symmetry. We refer the reader to \([4, 23, 24]\) for
surveys on circulant graphs in the context of network design with an emphasis on connectivity, diameter and efficiency in information dissemination. The reader may also consult [19, 27] for a survey on Cayley graphs as models for interconnection networks and an account of popular Cayley networks such as hypercubes, cube-connected cycles, star graphs, and so on.

A. COMPLETE ROTATIONS. Motivated by the need to construct fast gossiping algorithms, Bermond, Kodate and Pérennes introduced [5] the concept of complete rotation in Cayley graphs. (See §1.3 for terminology not defined in this subsection.) Among other things they proved [5, Corollary 15] that, if a Cayley graph with $n$ vertices and valency $d$ admits a complete rotation whose set of fixed points is empty, then its gossiping time under the store-and-forward, all-port and full-duplex model [5] is equal to the trivial lower bound $(n-1)/d$, which is the best one can hope for. They also proved [5, Lemma 17] that, if a Cayley graph admits a complete rotation whose fixed-point set is an independent set and not a vertex-cut, then its gossiping time is equal to $(n-1)/d$. (A vertex-cut of a graph is a subset of its vertex set whose removal increases the number of connected components.) They proved further that several popular network structures, including hypercubes, star graphs and multi-dimensional tori, admit complete rotations, and using this they determined the exact value of the gossiping time of these networks. In [15], Fragopoulou and Akl introduced a similar notion of rotation and used it to construct efficient communication algorithms. What is called a rotation of a Cayley graph in [15] is a complete rotation (as used in [5, 21] and the present paper) that is also an inner automorphism of the group defining the Cayley graph. Since complete rotations enable efficient and simple gossiping algorithms [5, 15], an interesting but challenging problem, as addressed in [5], is to classify or characterize Cayley graphs that admit a complete rotation. This problem was studied by Heydemann, Marlin and Pérennes in [21], where they gave among other things a few group-theoretic conditions for the existence of a complete rotation in a Cayley graph. For example, they proved [21, Corollary 3.1] that a connected Cayley graph Cay$(G, S)$ admits a complete rotation if and only if there exists a presentation $\langle S | R \rangle$ of $G$ such that the free group $F(S)$ has an automorphism that fixes $R$ and induces a cyclic permutation of $S$. Proving a conjecture of Bermond, Kodate and Pérennes [5], Lichiardopol [28] showed that the $k$-dimensional toroidal mesh with $n^k$ vertices (where $n \geq 3$) admits a complete rotation whose fixed-point set is not a vertex-cut. In the same paper, he also disproved a stronger conjecture by the same group [5] which asserts that the fixed-point set of any complete rotation of a Cayley graph is not a vertex-cut.

B. BALANCED REGULAR CAYLEY MAPS. It was observed in [29] that a complete rotation in a Cayley graph is a special skew-morphism [26], and that the existence of a complete rotation in a Cayley graph $\Gamma$ is equivalent to the existence of a 2-cell embedding of $\Gamma$ on a closed orientable surface as a balanced regular Cayley map [32]. Regular Cayley maps themselves are important objects of study in topological graph theory. In particular, from [26, 32] it is evident that constructions and/or characterizations of balanced regular Cayley maps are of considerable interest to the field of regular maps.

C. FROBENIUS GRAPHS AND HARTS (HEXAGONAL MESHES). In [39, Theorem 5.3], the second author proved that, if there exists a subgroup $H$ of the setwise stabilizer Aut$(G,S)$ of $S$ in Aut$(G)$ such that the union of the $H$-orbits on $G \setminus \{1\}$ of length less than $|H|$ is an independent set and not a vertex-cut of $\Gamma = Cay(G, S)$, then the gossiping time of $\Gamma$ is given by $(n-1)/d$. He also proved [39, Theorem 5.1] that the same result holds if there exists a subgroup $H \leq$ Aut$(G)$ that is regular on $S$ and semiregular on $G \setminus \{1\}$. Such graphs are
called the first-kind Frobenius graphs, and they were studied in [33, 16] and further investigated in [39] from a communication point of view. These two results in [39] generalize Lemma 17 and Corollary 15 in [5], respectively. In [39] Theorem 5.1] it was also proved that the first-kind Frobenius graphs admit ‘perfect’ optimal gossiping algorithms in some sense. Moreover, by [33, 16] and [39] Section 6], such graphs achieve the smallest possible edge-forwarding [20] and arc-forwarding indices [39] and also support ‘perfect’ routing schemes in a sense. It is thus desirable to classify, for example, the first-kind Frobenius circulants, and this has been achieved in [35] and [36] in the cases of valency 4 and 6, respectively. It turns out that these two families of circulants all admit complete rotations; see [35, Theorem 2] and [36, Theorem 2], respectively. Moreover, recently we became aware of the fact that a very special subfamily of first-kind Frobenius circulants of valency 6 had physically been used [10, 14] as multiprocessor interconnection networks at the Real-Time Computing Laboratory, The University of Michigan.

They are called HARTS (Hexagonal Architecture for Real-Time Systems) [14] or hexagonal mesh interconnection networks [2] in the computer science literature. The fact that the topological structures of HARTS are indeed some special first-kind Frobenius circulants of valency 6 was justified in [36]; see also [2, 3] in this paper. In the combinatorial community they were first studied in [35], and their optimal routing and gossiping algorithms were given in [39].

We refer the reader to [17, 40] for other recent results on Frobenius graphs, and to [22] for a survey on information dissemination in communication networks.

1.2 A summary of main results

From the above it should be clear that it would be interesting to classify all rotational Frobenius circulants and give a methodology for constructing them. We will achieve this in the present paper with the help of number theory; see Theorem [2, 7]. In view of (B) above, this can also be viewed as a classification of Frobenius circulants that are 2-cell embeddable on closed oriented surfaces as balanced regular Cayley maps (see Corollary [2, 9]). We will also study a family of rotational circulants with $p^e$ vertices, where $p$ is an odd prime and $e \geq 3$ an integer, and give a necessary and sufficient condition for the corresponding fixed-point set to be a non-vertex-cut; see Theorem [3, 1]. On the one hand, from this result we obtain a new family of rotational circulants whose gossiping time is equal to the aforementioned trivial lower bound. On the other hand, this result generalizes Lichiardopol’s single counterexample [28] to the conjecture of Bermond, Kodate and Pérennes [5] as mentioned in (A), to an infinite family of counterexamples.

1.3 Definitions

Let $G$ be a group with identity element 1, and let $V$ be a set. An action of $G$ on $V$ is a mapping $V \times G \to V, (v, g) \mapsto v^g$, such that $v^1 = v$ and $(v^g)^h = v^{gh}$ for $v \in V$ and $g, h \in G$. We use $v^G := \{v^g : g \in G\}$ to denote the $G$-orbit containing $v$ and $G_v := \{g \in G : v^g = v\}$ the stabilizer of $v$ in $G$. $G$ is semiregular on $V$ if $G_v = 1$ is the trivial subgroup of $G$ for all $v \in V$, transitive on $V$ if $v^G = V$ for some (and hence all) $v \in V$, and regular on $V$ if it is both transitive and semiregular on $V$. If a group $H$ acts on $G$ such that $(uv)^h = u^h v^h$ for any $u, v \in G$ and $h \in H$, then $H$ is said to act on $G$ as a group. In this case we use $G \rtimes H$ to denote the semidirected product [12] of $G$ by $H$ with respect to the action.

It is well known that a Cayley graph $\Gamma = \text{Cay}(G, S)$ has valency $|S|$, and it is connected if and only if $\langle S \rangle = G$. Since $(x, g) \mapsto x g, x, g \in G$, defines a regular action of $G$ on $G$ (as
a set) which preserves the adjacency of \( \Gamma \) (see e.g. [6]), we may view \( G \) as a subgroup of the automorphism group \( \text{Aut}(\Gamma) \) of \( \Gamma \). Define \( \text{Aut}(G, S) := \{ \alpha \in \text{Aut}(G) : S^\alpha = S \} \) to be the setwise stabilizer of \( S \) in \( \text{Aut}(G) \) under the natural action of \( \text{Aut}(G) \) on \( G \), and \( \text{Aut}(\Gamma)_1 \) the stabilizer of the vertex 1 in \( \text{Aut}(\Gamma) \). Then \( \text{Aut}(G, S) \leq \text{Aut}(\Gamma)_1 \) (see e.g. [18] or [6] Proposition 16.2).

A bijection \( \omega : G \to G \) is called \([5]\) a \textit{complete rotation} of \( \text{Cay}(G, S) \) if there exists an ordering of \( S = \{ s_0, s_1, \ldots, s_{d-1} \} \) (where \( d = |S| \)) such that \( \omega(1) = 1 \) and \( \omega(gs_i) = \omega(g)s_{i+1} \) for all \( g \in G \) and \( i = 0, 1, \ldots, d-1 \), with subscripts mod \( d \). In particular, \( \omega(s_i) = s_{i+1} \) for each \( i \) and so \( \omega \) permutes the elements of \( S \) cyclically. In [21] Proposition 2.2 it is shown that a bijection \( \omega : G \to G \) is a complete rotation of \( \text{Cay}(G, S) \) if and only if \( \omega \in \text{Aut}(G, S) \) and for some (and hence all) \( s \in S \), \( s^{(\omega)} = \{ s, s^{\omega}, s^{\omega^2}, \ldots, s^{\omega^{d-1}} \} = S \), where \( \langle \omega \rangle \) is the cyclic group generated by \( \omega \). An element \( g \in G \) is called a \textit{fixed point} of \( \omega \) if \( g \neq 1 \) and there exists \( i \in \{ 1, \ldots, d-1 \} \) such that \( g^{s^i} = g \). A Cayley graph is called \textit{rotational} if it admits a complete rotation.

An \textit{arc} of a graph is an ordered pair of adjacent vertices. A graph \( \Gamma \) is \( G \)-\textit{arc-transitive} if \( G \leq \text{Aut}(\Gamma) \) and \( G \) is transitive on the set of arcs of \( \Gamma \). \( \Gamma \) is \textit{arc-transitive} if it is \( \text{Aut}(\Gamma) \)-arc-transitive. It is easy to see that any rotational Cayley graph is arc-transitive.

Given a generating set \( S \) of a group \( G \) and a cyclic permutation \( \rho \) of \( S \), a \textit{Cayley map} \( M = \text{CM}(G, S, \rho) \) [26] [32] is a 2-cell embedding of the Cayley graph \( \text{Cay}(G, S) \) on an orientable surface such that for each vertex \( g \in G \), the cyclic permutation of the arcs \( (g, sg) \), \( s \in S \), induced by a fixed orientation of the surface coincides with \( \rho \). \( M \) is called \textit{balanced} [32] if \( \rho(s^{-1}) = \rho(s)^{-1} \) for every \( s \in S \), and \textit{regular} if its automorphism group is regular on the set of arcs of \( \text{Cay}(G, S) \).

A \textit{Frobenius group} \( G \) is a transitive group on a set \( V \) which is not regular on \( V \) such that the only element of \( G \) which fixes two points of \( V \) is the identity element of \( G \). It is well known (see e.g. [12] p.86) that a finite Frobenius group \( G \) has a nilpotent normal subgroup \( K \), called the \textit{Frobenius kernel}, which is regular on \( V \). Hence \( G = K \rtimes H \), where \( H \) is the stabilizer of a point of \( V \); each such group \( H \) is called a \textit{Frobenius complement} of \( K \) 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 may choose \( H \) to be the stabilizer of 1 so that \( H \) acts on \( K \) by conjugation. Obviously, \( H \) is semiregular on \( K \setminus \{ 1 \} \). Following [19] Theorem 1.4, a \textit{G-Frobenius graph} is a connected Cayley graph \( \text{Cay}(K, S) \) such that, for some \( a \in K \) with \( \langle a^H \rangle = K \), (i) \( S = a^H \) if \( |H| \) is even or \( a \) is an involution, or (ii) \( S = a^H \cup (a^{-1})^H \) if \( |H| \) is odd and \( a \) is not an involution. Hereinafter \( x^H := \{ h^{-1}xh : h \in H \} \) is the \( H \)-orbit containing \( x \in K \) under the action of \( H \) on \( K \) (by conjugation). Since \( G \) is a Frobenius group, \( H \) may be regarded as a subgroup of \( \text{Aut}(K) \). Thus \( H \leq \text{Aut}(K, S) \leq \text{Aut}(\Gamma)_1 \) and consequently \( G \leq \text{Aut}(\Gamma) \). We call \( \text{Cay}(K, S) \) a \textit{first-kind} or \textit{second-kind} \( G \)-Frobenius graph [39] according as whether \( S \) is given by (i) or (ii).

We refer the reader to [7], [12] and [8, 25, 31] for graph, group and number-theoretic terminology and notation, respectively.

## 2 Classification of rotational first-kind Frobenius circulants

### 2.1 Preparations

In this subsection we collect several preliminary results that will be used in the proof of our main results.

Let \( \mathbb{Z}_n \) be the additive group of integers mod \( n \), where \( n \geq 3 \) is an integer. Let \( \mathbb{Z}_n^* = \{ [u] : 1 \leq u \leq n-1, \gcd(n, u) = 1 \} \) be the multiplicative group of units of the ring \( \mathbb{Z}_n \). Here
the residue classes \([u]\) are mod \(n\), and we may write \([u]_n\) in place of \([u]\) if there is a danger of confusion. We have \(\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*\) 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 \([u] \in \mathbb{Z}_n^*\). Thus, for a subgroup \(H\) of \(\mathbb{Z}_n^*\), \(\mathbb{Z}_n \rtimes H\) inherits from \(\mathbb{Z}_n \rtimes \mathbb{Z}_n^*\) the same action on \(\mathbb{Z}_n\). We use \([u]^{-1}\) to denote the inverse element of \([u]\) in \(\mathbb{Z}_n^*\), and \([u]\) to denote the cyclic subgroup of \(\mathbb{Z}_n^*\) generated by \([u]\). The operation of \(\mathbb{Z}_n \rtimes \mathbb{Z}_n^*\) is defined by \(([x_1],[u_1])([x_2],[u_2]) = ([x_1]+[x_2][u_1]^{-1},[u_1][u_2])\) 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 \((-[xu],[u]^{-1})\).

The first statement in the following lemma was proved in [21, Lemma 3.1], and the second one can be verified easily.

**Lemma 2.1.** Let \(\Gamma = \text{Cay}(\mathbb{Z}_n,S)\) be a connected circulant graph of valency \(d = |S|\). Then \(\Gamma\) admits an element of \(\mathbb{Z}_n^*\) as a complete rotation if and only if there exist integers \(h\) and \(s\) both coprime to \(n\) such that \(S = \{[sh^i] : i = 1, \ldots , d\}\) and \(h\) has order \(d\) mod \(n\). Moreover, in this case we have \(\Gamma \cong \text{Cay}(\mathbb{Z}_n,S')\), where \(S' = \langle [h] \rangle = \{[h^i] : i = 1, \ldots , d\}\), and \([sx] \mapsto [x]\) is an isomorphism between the two graphs.

Thus a circulant graph of \(n\) vertices admits \([h] \in \mathbb{Z}_n^*\) as a complete rotation if and only if it is isomorphic to \(\text{Cay}(\mathbb{Z}_n, \langle [h] \rangle)\) with \(\langle [h] \rangle\) closed under inverse elements.

It is easy to see [39, Section 2] that a connected Cayley graph \(\text{Cay}(G,S)\) is a first-kind \(G \rtimes H\)-Frobenius graph if and only if \(H \leq \text{Aut}(G)\) is regular on \(S\) and semiregular on \(G \setminus \{1\}\).

When \(G = \mathbb{Z}_n\), this yields:

**Lemma 2.2.** Let \(\Gamma = \text{Cay}(\mathbb{Z}_n,S)\) be a connected circulant graph.

(a) If there exists a subgroup \(H\) of \(\mathbb{Z}_n^*\) that is regular on \(S\) and semiregular on \(\mathbb{Z}_n \setminus \{0\}\), then \(\mathbb{Z}_n \rtimes H\) is a Frobenius group and \(\Gamma\) is a first-kind \(\mathbb{Z}_n \rtimes H\)-Frobenius graph.

(b) Conversely, if \(\Gamma\) is a first-kind \(\mathbb{Z}_n \rtimes H\)-Frobenius graph, where \(H\) is a subgroup of \(\mathbb{Z}_n^*\) such that \(\mathbb{Z}_n \rtimes H\) is a Frobenius group, then \(H\) is regular on \(S\) and semiregular on \(\mathbb{Z}_n \setminus \{0\}\).

It can happen that a circulant \(\Gamma\) is isomorphic to some \(K \rtimes H\)-Frobenius graph \(\text{Cay}(K,S)\), but \(K\) is not a cyclic group and \(H\) is not regular on \(S\). For example, if \(n = p^e\) is a prime power with \(e \geq 2\), then \(G = \mathbb{Z}_{p^e}^* \rtimes \mathbb{Z}_{p-1}^* \cong \text{AGL}(1,n)\) is a Frobenius group and the complete graph \(K_n = \text{Cay}(\mathbb{Z}_{p^e},\mathbb{Z}_{p^e}^* \setminus \{0\})\) is a \(G\)-Frobenius graph. This describes \(K_n\) as a Cayley graph on a non-cyclic group. Note that \(K_n\) is not a \(\mathbb{Z}_n \rtimes H\)-Frobenius graph for any \(H \leq \mathbb{Z}_n^*\), because \(\mathbb{Z}_n^*\) cannot have any subgroup regular on \(\mathbb{Z}_n \setminus \{0\}\).

In the sequel we focus on the first-kind Frobenius circulants such that the underlying Frobenius group \(\mathbb{Z}_n \rtimes H\) has kernel \(\mathbb{Z}_n\). Slightly abusing terminology, we say that such a circulant has kernel \(\mathbb{Z}_n\) and complement \(H\).

**Lemma 2.3.** Let \(\Gamma\) be a first-kind Frobenius circulant with kernel \(\mathbb{Z}_n\). Then \(n\) is odd and \(\Gamma\) has even valency.

**Proof.** Let \(\Gamma = \text{Cay}(\mathbb{Z}_n,S)\) be a first-kind \(\mathbb{Z}_n \rtimes H\)-Frobenius circulant. Then \(H\) is regular on \(S\) and semiregular on \(\mathbb{Z}_n \setminus \{0\}\) by Lemma 2.2. Hence \(|H| = |S|\) and \(|H|\) divides \(n-1\).

Suppose the valency \(|S|\) of \(\Gamma\) is odd. Then \(|H|\) is odd and thus by the definition of a first-kind Frobenius graph, \(S = [x]^H\) for an involution \([x] \in \mathbb{Z}_n\). Since \([x]\) is an involution, so is every element of \(S\). Since \(\mathbb{Z}_n\) contains at most one involution, it follows that \(|S| = 1\) and so \(\Gamma\) is a
disconnected graph. This contradiction shows that \(|S|\) must be even, which implies that \(n\) must be odd as \(|S|\) is a divisor of \(n - 1\).

Lemma 2.4. (35, 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 every \([h] \in H \setminus \{[1]\}\).

The following is a refinement of Lemma 2.4 in the case when \(H\) is cyclic. Given coprime integers \(m\) and \(a\), we say that \(a\) has order \(k\) mod \(m\) if \(a \pmod{m}\) has order \(k\) in \(\mathbb{Z}_m^*\).

Lemma 2.5. Let \(H = \langle [h]\rangle\) be a cyclic subgroup of \(\mathbb{Z}_n^*\) with order \(|H| = d\) (where \(1 \leq h \leq n - 1\)). Then \(H\) is semiregular on \(\mathbb{Z}_n \setminus \{[0]\}\) if and only if for every prime factor \(p\) of \(n\), \(h\) has order \(d\) mod \(p\).

Proof. Suppose that \(H\) is semiregular on \(\mathbb{Z}_n \setminus \{[0]\}\). Then by Lemma 2.4 we have \(\gcd(h^i - 1, n) = 1\) for \(i = 1, \ldots, d - 1\). Consequently, for \(i = 1, \ldots, d - 1\) and each prime factor \(p\) of \(n\), we have \(\gcd(h^i - 1, p) = 1\) and so \(h\) does not have order \(i\) mod \(p\). On the other hand, since \(H\) is cyclic of order \(d\), we have \(h^d \equiv 1 \pmod{n}\) and so \(h^d \equiv 1 \pmod{p}\). Therefore, for each prime factor \(p\) of \(n\), \(h\) has order \(d\) mod \(p\).

Conversely, suppose that \(h\) has order \(d\) mod \(p\) for every prime factor \(p\) of \(n\). Then \(h^i - 1 \neq 0 \pmod{p}\) and so \(\gcd(h^i - 1, p) = 1\) for \(i = 1, \ldots, d - 1\). Since this holds for every prime factor \(p\) of \(n\), we have \(\gcd(h^i - 1, n) = 1\) for \(i = 1, \ldots, d - 1\). This together with Lemma 2.4 implies that \(H\) is semiregular on \(\mathbb{Z}_n \setminus \{[0]\}\).

A subset \(S\) of a finite group \(G\) is called \([30]\) a CI-subset of \(G\) if for every subset \(S'\) of \(G\), \(\text{Cay}(G, S)\) and \(\text{Cay}(G, S')\) are isomorphic if and only if \(S' = S^\sigma\) for some \(\sigma \in \text{Aut}(G)\). It was proved by Muzychuk, Klin and Pöschel [30 Theorem 5.2], and Dobson and Morris [13] independently, that every \(S \subset \mathbb{Z}_n^*\) is a CI-subset of \(\mathbb{Z}_n^*\).

Lemma 2.6. Let \(\Gamma = \text{Cay}(\mathbb{Z}_n, S)\) and \(\Gamma' = \text{Cay}(\mathbb{Z}_n, S')\) be rotational first-kind Frobenius circulants such that the underlying Frobenius groups have kernel \(\mathbb{Z}_n\) and complements \(H, H' \leq \mathbb{Z}_n^*\), respectively. Then \(\Gamma\) and \(\Gamma'\) are not isomorphic unless \(H = H'\).

Proof. By Lemma 2.4 we may assume \([1] \in S\) without loss of generality. Since by Lemma 2.2 \(H\) is regular on \(S\), we have \(S = H\) (as sets). Similarly, we may assume \([1] \in S'\) so that \(S' = H'\).

Assume \(\Gamma \cong \Gamma'\). Then \(\sigma S = S'\) for some \(\sigma \in \mathbb{Z}_n^*\) by the aforementioned result of [30]. Since \(S = H\) and \(S' = H'\), we have \(\sigma H = H'\). Since \([1] \in H'\), there exists \([h] \in H\) such that \(\sigma[h] = [1]\), that is, \([h]\) is the inverse of \(\sigma\) in \(\mathbb{Z}_n^*\). Since \([h]\) is in \(H\), so is \(\sigma\), and hence \(H' = \sigma H = H\).

2.2 Classification

The main result in this section is Theorem 2.7 below, which both classifies rotational first-kind Frobenius circulants with kernel \(\mathbb{Z}_n\), and describes a means to construct them. In the proof of this result we will use the fact that for any odd prime \(p\) and any integer \(e \geq 1\), a primitive root mod \(p^e\) is also a primitive root mod \(p\). (In fact, for a primitive root \(\eta\) mod \(p^e\) and every \(a \in \{1, \ldots, p - 1\}\), there exists an integer \(m\) such that \(\eta^m \equiv a \pmod{p^e}\). Hence \(\eta^m \equiv a \pmod{p}\) and \(\eta\) generates \(\mathbb{Z}_p^*\). Denote by \(\varphi\) Euler’s totient function.

Theorem 2.7. Let \(n = p_1^{e_1} \cdots p_l^{e_l}\) be a positive integer in canonical prime factorization. Let \(D = \gcd(p_1 - 1, \ldots, p_l - 1)\). There exists a rotational first-kind Frobenius circulant with kernel \(\mathbb{Z}_n\) and valency \(d\) if and only if \(n\) is odd and \(d\) is an even divisor of \(D\).
Moreover, if \( n \) is odd and \( d \) is an even divisor of \( D \), then there are precisely \( \varphi(d)^{l-1} \) pairwise non-isomorphic rotational first-kind Frobenius circulants of valency \( d \) with kernel \( \mathbb{Z}_n \). Each of these circulants is isomorphic to \( \text{Cay}(\mathbb{Z}_n, \{[h]\}) \) for some \([h] \in \mathbb{Z}_n^* \) of the form

\[
h = \sum_{i=1}^{l} \frac{n}{p_i^e} b_i h_i,
\]

where \( b_i \) and \( h_i \) are integers satisfying

\[
b_i (n/p_i^e) \equiv 1 \pmod{p_i^e}
\]

and

\[
h_i \equiv \eta_{i}^{m_i \varphi(p_i^e)/d} \pmod{p_i^e}
\]

for a fixed primitive root \( \eta_i \) \( \pmod{p_i^e} \) and an integer \( m_i \) coprime to \( d \). Furthermore, each such circulant is a first-kind \( \mathbb{Z}_n \times \mathbb{Z}_d \)-Frobenius graph that admits \([h]\) above as a complete rotation.

**Proof.** CONSTRUCTION: Let \( n \) be odd, and \( d \) an even divisor of \( D \). We prove that the circulants described in the final portion of the theorem are rotational first-kind Frobenius circulants with kernel \( \mathbb{Z}_n \) and valency \( d \). For each \( i \in \{1, \ldots, l\} \), let \( \eta_i \) be a primitive root \( \pmod{p_i^e} \), that is, \( \eta_i \) is a generator of the cyclic group \( \mathbb{Z}_{p_i^e}^* \). Since \( d \) is a divisor of \( p_i - 1 \), it is also a divisor of \( \varphi(p_i^e) = p_i^{e-1}(p_i - 1) \). Thus \( \eta_i^{\varphi(p_i^e)/d} \) generates the unique subgroup of \( \mathbb{Z}_{p_i^e}^* \) with order \( d \). Consequently, all generators of this subgroup have the form

\[
h_i = \eta_i^{m_i \varphi(p_i^e)/d}
\]

for an integer \( m_i \) coprime to \( d \). It is easily seen that \( h_i \) has order \( d \pmod{p_i^e} \). Therefore, \( h_i^d \equiv 1 \pmod{p_i^e} \).

Set

\[
h = \sum_{i=1}^{l} \frac{n}{p_i^e} b_i h_i,
\]

where the integer \( b_i \) satisfies \( b_i (n/p_i^e) \equiv 1 \pmod{p_i^e} \) (that is, \( b_i \) is the inverse element of \( n/p_i^e \) in \( \mathbb{Z}_{p_i^e}^* \)) and \( h_i \) is as above. As detailed in [31, Section 2.5], the Chinese Remainder Theorem implies that \( h \) satisfies \( h^d \equiv 1 \pmod{n} \). Moreover, for each \( i \in \{1, \ldots, l\} \), \( h \) satisfies \( h \equiv h_i \pmod{p_i^e} \). Thus \( h \) has order \( d \pmod{p_i^e} \), and therefore \( h \) has order \( d \pmod{n} \).

We now use \( h \) above to construct a rotational circulant graph. Define \( H = \langle [h]\rangle \). Then \( H \) is a cyclic subgroup of \( \mathbb{Z}_n^* \) of order \( d \). Let \( S = H \) (as sets). We claim that \( S \) is a connection set of \( \mathbb{Z}_n \) and hence defines a circulant. To justify this it suffices to show \([-1] \in S \) (note that \([0] \not\in S\)). In fact, since \( d \) is even, we can write \( d = 2k \), where \( k \) is a positive integer. The cyclic group \( \mathbb{Z}_{p_i^e}^* \) contains a unique involution, namely, \( \eta_i^{\varphi(p_i^e)/2} \equiv -1 \pmod{p_i^e} \). Note that \( m_i \) must be odd because it is coprime to the even integer \( d \). Since \( k = d/2 \), we have \( h^k \equiv h_i^{k} \equiv \eta_i^{m_i \varphi(p_i^e)/2} \equiv -1 \pmod{p_i^e} \), and consequently \( h^k \equiv -1 \pmod{n} \). Since \([h] \in S\), it follows that \([-1] \in S \) and so \( S = -S \). Therefore, \( \Gamma = \text{Cay}(\mathbb{Z}_n, S) \) is a well-defined circulant graph of valency \( |S| = d \). It is evident that \( H \) is regular on \( S \) and \( \Gamma \) admits \([h]\) as a complete rotation.

Next we show that \( H \) is semiregular on \( \mathbb{Z}_n \setminus [0] \). As noted above, for each \( i \in \{1, \ldots, l\} \), \( h \) satisfies \( h \equiv h_i \pmod{p_i^e} \) and has order \( d \pmod{p_i^e} \). Note that \( h_i \equiv \eta_i^{m_i \varphi(p_i^e)/d} \equiv \eta_i^{m_i (p_i^e-1)} \pmod{d} \).
(mod \( p_i \)). Note also that \( \eta_i \) is a primitive root mod \( p_i \) because it is a primitive root mod \( p_i^{e_i} \). Thus \( \eta_i \) has order \( p_i - 1 \mod p_i \) and consequently \( \eta_i^{p_i-1} \equiv \eta_i \mod p_i \). Therefore, \( h_i \equiv \eta_i^{m_i(p_i-1)/d} \mod p_i \). Since \( d \) is a divisor of \( p_i - 1 \), \( \eta_i^{(p_i-1)/d} \mod \) has order \( d \mod p_i \); in other words, \( \eta_i^{(p_i-1)/d} \mod \) generates the unique subgroup of \( \mathbb{Z}_{p_i}^* \) of order \( d \). Since \( \gcd(m_i, d) = 1 \), we deduce that \( \eta_i^{m_i(p_i-1)/d} \mod \) also has order \( d \mod p_i \). Since \( h_i \equiv \eta_i^{m_i(p_i-1)/d} \mod p_i \), this means that \( h_i \) has order \( d \mod p_i \). Therefore, \( h_i \equiv h_i \mod (p_i) \) has order \( d \mod p_i \) for each \( i \in \{1, \ldots, l\} \). It then follows from Lemma 2.5 that \( H \) is semiregular on \( \mathbb{Z}_n \setminus \{0\} \). Finally, since \( H \equiv \mathbb{Z}_d \), we conclude that \( \Gamma \) is a first-kind \( \mathbb{Z}_n \times \mathbb{Z}_d \)-Frobenius graph of order \( d \) that admits \([h]\) as a complete rotation.

Completeness of construction: We have already seen in Lemma 2.3 that no first-kind Frobenius circulants with kernel \( \mathbb{Z}_n \) exist when \( n \) is even.

We now show that, up to isomorphism, every rotational first-kind Frobenius circulant with kernel \( \mathbb{Z}_n \) arises from the construction above. Let \( \Gamma = \text{Cay}(\mathbb{Z}_n, S) \) be such a circulant with valency \( |S| = d \), where \( n \) is odd. Then by Lemma 2.2 there exists a subgroup \( H \) of \( \mathbb{Z}_n^* \) that is regular on \( S \) and semiregular on \( \mathbb{Z}_n \setminus \{0\} \) such that \( \Gamma \) is a \( \mathbb{Z}_n \times H \)-Frobenius graph. Moreover, as we saw in the proof of Lemma 2.2 we may assume without loss of generality that \( S = H = \{[h]\} \) (as sets), where \([h]\) is a complete rotation of \( \Gamma \). Thus \( h \) has order \( d \mod n \), and \( d \) must be even by Lemma 2.3. Since \( H \) is semiregular on \( \mathbb{Z}_n \setminus \{0\} \), by Lemma 2.5 for each \( i \in \{1, \ldots, l\} \), \( h \) has order \( d \mod p_i \) and consequently \( d \) divides \( |\mathbb{Z}_{p_i}^*| = p_i - 1 \). Since this holds for every \( i \), it follows that \( d \) divides \( D \). Moreover, \( h \) also has order \( d \mod p_i^{e_i} \) for each \( i \in \{1, \ldots, l\} \). This is because the order of \( h \mod p_i^{e_i} \) is bounded above by the order of \( h \mod n \), and below by the order of \( h \mod p_i \), but both bounds are equal to \( d \). Since the unique subgroup of \( \mathbb{Z}_{p_i^{e_i}}^* \) with order \( d \) is generated by \( \eta_i^{\varphi(p_i^{e_i})/d} \mod p_i^{e_i} \), where \( \eta_i \) is a primitive root mod \( p_i^{e_i} \), without loss of generality we may assume \( h \equiv \eta_i^{m_i\varphi(p_i^{e_i})/d} \mod p_i^{e_i} \), where \( m_i \) is an integer coprime to \( d \). As shown in Section 2.5, by the Chinese Remainder Theorem, \( h \) has expression (1) with \( b_i \) and \( h_i \) as given in (2) and (3), respectively.

Enumeration: We now enumerate all possible \( h \) in (1) and determine when the corresponding first-kind Frobenius circulants are isomorphic. Since each \( \mathbb{Z}_{p_i^{e_i}}^* \) has exactly one subgroup of order \( d \), without loss of generality we may fix the primitive root \( \eta_i \) in (3). There are exactly \( \varphi(d) \) values \( h_i \) as in (3), and each of them corresponds to a different value of \( m_i \). Since this is true for each \( i \in \{1, \ldots, l\} \) and since each \( b_i \) (mod \( p_i^{e_i} \)) is unique, we conclude that there are exactly \( \varphi(d)^l \) different possibilities for \( h \).

We now demonstrate that different choices of \( h \) can generate the same group \( H \) in \( \mathbb{Z}_n^* \). Since \( H \) is cyclic of order \( d \), it has exactly \( \varphi(d) \) generators. We claim that each of them corresponds to a different \( h \) in (1). Let \( h_0 \) be a fixed solution to (1) corresponding to positive integers \( m_i \) coprime to \( d \). Then by (1) and (3), we have \( h_0 \equiv \eta_i^{m_i\varphi(p_i^{e_i})/d} \mod p_i^{e_i} \) for each \( i \in \{1, \ldots, l\} \). Let \( m_j \) be a positive integer coprime to \( d \). Then \( h_0 \equiv \eta_i^{m_j\varphi(p_i^{e_i})/d} \mod p_i^{e_i} \). Since \( m_im_j \) is coprime to \( d \), a possible value for \( h_i \) in (3) is \( h_i \equiv \eta_i^{m_j\varphi(p_i^{e_i})/d} \mod p_i^{e_i} \). Therefore, \( h = h_0 \) is also a solution to (1). However, \( h_0 \) and \( h_0^{m_j} \) generate the same subgroup \( H \) of \( \mathbb{Z}_n^* \), and therefore the same first-kind \( \mathbb{Z}_n \times H \)-Frobenius circulant \( \Gamma \). (Recall that the connection set for \( \Gamma \) is defined by \( S = H \) in our construction.) In other words, if \( \Gamma \) is a rotational first-kind \( \mathbb{Z}_n \times H \)-Frobenius circulant of order \( d \), then \( H \) has \( \varphi(d) \) generators, and each of them is a different solution \( h \) to (1). Since there are \( \varphi(d)^l \) possible values for \( h \), we deduce that there are at most \( \varphi(d)^{l-1} \)
rotational first-kind Frobenius circulants of valency \(d\) with kernel \(\mathbb{Z}_n\). However, by Lemma 2.6 different subgroups \(H\) give rise to non-isomorphic circulants. Therefore, there are exactly \(\varphi(d)^{l-1}\) rotational first-kind Frobenius circulants of valency \(d\) with kernel \(\mathbb{Z}_n\).

The valency \(d\) of \(\text{Cay}(\mathbb{Z}_n, (|h|))\) in Theorem 2.7 is strictly less than the smallest prime divisor of \(n\). In particular, if 3 is a divisor of \(n\), then \(d = 2\) and so the only rotational first-kind Frobenius circulant with kernel \(\mathbb{Z}_n\) is the cycle of length \(n\).

We illustrate Theorem 2.7 by the following example.

Example 2.8. Let \(n = 6253 = 13^2 \times 37\), so that \(p_1 = 13\), \(p_2 = 37\), and \(D = \gcd(12, 36) = 12\). Choose \(\eta_1 = \eta_2 = 2\), which is a primitive root mod 13 as well as a primitive root mod 37. By [2], we have \(b_1 \equiv 37^{-1} \equiv 32 \pmod{13^2}\) and \(b_2 \equiv (13^2)^{-1} \equiv 30 \pmod{37}\).

The even divisors of \(D\) are \(d = 2, 4, 6\) and \(12\), and respectively, they produce \(\varphi(d) = 1, 2, 2\) and 4 non-isomorphic rotational first-kind Frobenius circulants \(\text{Cay}(\mathbb{Z}_{6253}, h)\) with kernel \(\mathbb{Z}_{6253}\). These circulants are listed in Table 1, omitting the pairs \((m_1, m_2)\) that produce a circulant isomorphic to one already in the table.

In view of (B) in [1] Theorem 2.7 can be restated as follows.

Corollary 2.9. Let \(n = p_1^{e_1} \ldots p_k^{e_k}\) be a positive integer in canonical prime factorization. Let \(D = \gcd(p_1 - 1, \ldots, p_k - 1)\). A first-kind Frobenius circulant \(\Gamma\) of valency \(d\) with kernel \(\mathbb{Z}_n\) can be embedded on a closed orientable surface as a balanced regular Cayley map if and only if (i) \(n\) is odd and \(d\) is an even divisor of \(D\), and (ii) \(\Gamma\) is isomorphic to a circulant constructed in Theorem 2.7.

Corollary 2.10. Let \(p\) be an odd prime, and let \(e \geq 1\) and \(d \geq 2\) be integers. There exists a rotational first-kind Frobenius circulant on \(p^e\) vertices with valency \(d\) and kernel \(\mathbb{Z}_{p^e}\) if and only if \(d\) is an even divisor of \(p - 1\). Moreover, up to isomorphism such a circulant is unique for every even divisor \(d\) of \(p - 1\), namely \(\text{Cay}(\mathbb{Z}_{p^e}, \langle|\eta p^{e-1}(p-1)/d|\rangle)\), where \(\eta\) is a primitive root mod \(p^e\).

Proof. Using the notation in Theorem 2.7, we have \(l = 1\), \(D = p - 1\), and \(b_1 = 1\) in [2]. The result follows from Theorem 2.7 by noting \(\varphi(d)^{l-1} = 1\) for every even divisor \(d\) of \(p - 1\), and by choosing \(m_1 = 1\) in [3].

Table 1: All rotational first-kind Frobenius circulants with kernel \(\mathbb{Z}_{6253}\).

| \(d\) | \((m_1, m_2)\) | \((h_1, h_2)\) | \(h\) | \(S = H = \langle|h|\rangle\) |
|---|---|---|---|---|
| 2 | (1, 1) | (99, 31) | -1 | \{±1\} |
| 4 | (1, 3) | (99, 6) | -2436 | \{±1, ±2436\} |
| 4 | (1, 1) | (147, 27) | -1712 | \{±1, ±1712, ±1713\} |
| 6 | (5, 5) | (147, 11) | -1543 | \{±1, ±1543, ±1544\} |
| 12 | (1, 1) | (80, 8) | -2286 | \{±1, ±746, ±1540, ±1712, ±1713, ±2286\} |
| 12 | (1, 5) | (80, 23) | -1272 | \{±1, ±526, ±746, ±1272, ±1543, ±1544\} |
| 12 | (1, 7) | (80, 29) | -2117 | \{±1, ±319, ±1712, ±1713, ±2117, ±2436\} |
| 12 | (1, 11) | (80, 14) | +3122 | \{±1, ±695, ±1543, ±1544, ±2436, ±3122\} |

9
In the special case when $e = 1$, Corollary 2.10 gives the following: there exists a rotational first-kind Frobenius circulant on $p$ vertices with valency $d$ and kernel $\mathbb{Z}_p$ if and only if $d$ is an even divisor of $p - 1$; in this case such a circulant is unique and is isomorphic to $\text{Cay}(\mathbb{Z}_p, ([\eta^{p-1}/d]])$, where $\eta$ is a primitive root mod $p$. It can be verified that this graph is in fact the unique first-kind Frobenius circulant on $p$ vertices with valency $d$ and kernel $\mathbb{Z}_p$. The family of such circulants $\text{Cay}(\mathbb{Z}_p, ([p^{p-1}/d]])$, with $d$ running over all even divisors of $p - 1$, is precisely the family of all arc-transitive graphs on $p$ vertices as classified in [9]. Thus we have:

**Corollary 2.11.** All arc-transitive graphs of prime order are rotational first-kind Frobenius circulants.

It follows from [34] Theorem 2 and [36] Theorem 2, respectively, that all first-kind Frobenius circulants of valency 4 or 6 are rotational. It would be interesting to explore if this extends to some other valencies.

### 2.3 HARTS, or hexagonal meshes

We now explain that HARTS (Hexagonal Architecture for Real-Time Systems), also known as hexagonal mesh, C-wrapped hexagonal mesh or hexagonal interconnection network, belongs to the family [36] of first-kind Frobenius circulants with kernel $\mathbb{Z}_n$ and valency 6, which in turn is a subfamily of the family of rotational circulants as classified in Theorem 2.7. HARTS was proposed [10] as a distributed real-time computing system, and its properties were studied in [10, 11, 2].

By [36] Theorem 2, a first-kind Frobenius circulant with kernel $\mathbb{Z}_n$ and valency 6 exists if and only if every prime factor of $n$ is congruent to 1 mod 6, and moreover such circulants are precisely $\text{Cay}(\mathbb{Z}_n, ([a]_n))$ with $a$ running over all solutions to the congruence equation $x^2 - x + 1 \equiv 0 \pmod{n}$. In particular, if $n_k = 3k^2 + 3k + 1$ where $k \geq 2$ is an integer, then $3k + 2$ is a solution to $x^2 - x + 1 \equiv 0 \pmod{n_k}$. Hence

$$TL_{n_k} := \text{Cay}(\mathbb{Z}_{n_k}, ([3k + 2]_{n_k})) = \text{Cay}(\mathbb{Z}_{n_k}, \{\pm[1]_{n_k}, \pm[3k + 1]_{n_k}, \pm[3k + 2]_{n_k}\})$$

is a first-kind Frobenius circulant with valency 6; see [34] and [36] Example 1. In [36], it was proved that $TL_{n_k}$ has diameter $k$, and among all circulants $\text{Cay}(\mathbb{Z}_n, \{\pm[a]_n, \pm[b]_n, \pm[c]_n\})$ of valency 6 and diameter $k$ such that $a + b + c \equiv 0 \pmod{n}$, $TL_{n_k}$ has the maximum number of vertices.

The HARTS $H_k$ of size $k$ has diameter $k - 1$ and $n_{k-1} = 3k^2 - 3k + 1$ vertices, and is isomorphic [10, 2] to the circulant $\text{Cay}(\mathbb{Z}_{n_{k-1}}, S)$ with $S = \{\pm[k-1]_{n_{k-1}}, \pm[k]_{n_{k-1}}, \pm[2k-1]_{n_{k-1}}\}$. Clearly, $[3k]_{n_{k-1}} \in \mathbb{Z}_{n_{k-1}}^*$. Thus $\text{Cay}(\mathbb{Z}_{n_{k-1}}, S) \cong \text{Cay}(\mathbb{Z}_{n_{k-1}}, S')$ via the isomorphism $[x]_{n_{k-1}} \mapsto [3k]_{n_{k-1}}[x]_{n_{k-1}}$, where $S' = \{\pm[k]_{n_{k-1}}[k-1]_{n_{k-1}}, \pm[3k]_{n_{k-1}}[k]_{n_{k-1}}, \pm[3k]_{n_{k-1}}[2k-1]_{n_{k-1}}\} = \{\pm[1]_{n_{k-1}}, \pm[3k-1]_{n_{k-1}}, \pm[3k-2]_{n_{k-1}}\}$. It follows that $H_k$ is isomorphic to $TL_{n_{k-1}}$.

The same conclusion can also be drawn as follows: $H_k$ is isomorphic [2] to the EJ network $EJ_{k+(k-1)\omega}$ where $\omega = (1 + \sqrt{3})/2$, but any EJ network $EJ_{a+bi}$ with $\gcd(a, b) = 1$ is isomorphic [36] Theorem 5] to a first-kind Frobenius circulant of valency 6.

### 3 A family of rotational non-Frobenius circulants

The purpose of this section is to prove the following result.

---

10
Theorem 3.1. Let \( q = p^e \) with \( p \) an odd prime and \( e \geq 3 \) an integer. Let
\[
\Gamma_{q,r} = \text{Cay}(\mathbb{Z}_q, [(p-1)p^r]),
\] (4)
where \( r \) is an integer between 0 and \( e-1 \). Then \( \Gamma_{q,r} \) is a connected rotational circulant of valency \( 2p^{e-r-1} \) that admits \( [(p-1)p^r] \) as a complete rotation. The set of fixed points of \( [(p-1)p^r] \) is equal to \( F = \{px \neq [0] : x \in \mathbb{Z} \} \) and is an independent set of \( \Gamma_{q,r} \). Moreover, \( F \) is a vertex-cut of \( \Gamma_{q,r} \) if and only if \( r \neq 0 \).

The circulants \( \Gamma_{q,r} \) above cannot be Frobenius, for otherwise the fixed-point set of \( [(p-1)p^r] \) would be empty. Note that the fixed-point set \( F \) of \( \Gamma_{q,r} \) does not rely on \( r \). Note also that \( \Gamma_{q,e-1} \) is isomorphic to the cycle of \( q \) vertices.

As mentioned in the introduction, it was proved in [5, Lemma 17] that if a Cayley graph has a complete rotation such that the corresponding fixed-point set is an independent set and not a vertex-cut, then its gossiping time can be easily computed. It is known [5] that some popular networks, including hypercubes, star graphs and multi-dimensional tori, have this property. Theorem 3.1 shows that \( \{\Gamma_{q,0} : q = p^e, p \text{ an odd prime, } e \geq 3\} \) is a new family of rotational Cayley graphs with this property. It was conjectured in [5] that the fixed-point set of any complete rotation of a Cayley graph is not a vertex-cut. Lichardopol [28] disproved this by a counterexample. Theorem 3.1 generalizes his construction to an infinite family of counterexamples, namely \( \Gamma_{q,r} \) with \( 1 \leq r \leq e-1 \). In fact, the counterexample in [28, Section 4] is exactly \( \Gamma_{3^n,1} \).

An immediate consequence of Theorem 3.1 and [5, Lemma 17] is that, for any odd prime \( p \) and integer \( e \geq 3 \), the gossiping time of \( \Gamma_{p^e,0} \) is equal to \( \lceil (p^e - 1)/2p^{e-1} \rceil \), which is quite small compared with the order \( p^e \) of \( \Gamma_{p^e,0} \).

3.1 Fixed points of a complete rotation

Before proving Theorem 3.1 let us briefly discuss basic properties of the fixed-point set of a complete rotation in a rotational Cayley graph.

Let \( \Gamma = \text{Cay}(G, S) \) be rotational with a complete rotation \( \omega \). Let \( H = \langle \omega \rangle \leq \text{Aut}(G) \). Then \( H \) is regular on \( S \) and permutes the elements of \( S \) in a cyclic manner. Define [39, Section 5]
\[
X(\omega) = \{x \in G : H_x = 1\} \cup \{1\},
\]
where \( H_x \) is the stabilizer of \( x \) in \( H \). Denote by \( F(\omega) \) the set of fixed points of \( \omega \). Denote by \( \Gamma - F(\omega) \) the graph obtained from \( \Gamma \) by deleting all vertices of \( F(\omega) \).

The first two parts of the following lemma were observed in [39, Section 5] under a general setting. We give their proofs for completeness of the present paper.

Lemma 3.2. With the notation above, we have:

(a) \( F(\omega) = G \setminus X(\omega) \);
(b) \( X(\omega) \setminus \{1\} \) is the union of all \( H \)-orbits on \( G \setminus \{1\} \) with length \( |S| \);
(c) \( F(\omega) \) is the union of all other \( H \)-orbits on \( G \setminus \{1\} \), that is, the union of all \( H \)-orbits whose lengths properly divide \( |S| \);
(d) $F(\omega)$ is not a vertex-cut of $\Gamma$ if and only if for every $H$-orbit $x^H$ contained in $X(\omega)$, there exists a path of $\Gamma - F(\omega)$ from 1 to at least one vertex of $x^H$.

Proof. Denote $d = |S|$.

(a) Let $x \in G$. We have: $x \in F(\omega) \iff x \neq 1$ and there exists $i \in \{1, \ldots, d - 1\}$ such that $x^\omega = x \iff x \neq 1$ and there exists $i \in \{1, \ldots, d - 1\}$ such that $\omega^j \in H_x \iff x \neq 1$ and $H_x \neq 1 \iff x \in G \setminus X(\omega)$.

(b) Since $H_x h = h^{-1} H_x h$ for any $x \in G \setminus \{1\}$ and $h \in H$, $H_x = 1$ if and only if $H_x h = 1$. Thus $X(\omega) \setminus \{1\}$ is invariant under $H$ and hence is the union of some $H$-orbits on $G \setminus \{1\}$. By the orbit-stabilizer lemma, an $H$-orbit on $G \setminus \{1\}$ is contained in this union if and only if it has length $d$.

(c) It can be verified that $F(\omega)$ is invariant under the action of $H$. (In fact, if $x \in F(\omega)$, then there exists $i \in \{1, \ldots, d - 1\}$ such that $x^\omega = x$. Thus, for any integer $j$, we have $(x^\omega)^j = x^\omega$ and so $x^\omega$ is not a vertex-cut of $x^H$.)

(d) The necessity is obvious. To prove the sufficiency, if a path as stated exists, then there exists a path of $\Gamma - F(\omega)$ from 1 to every vertex of $x^H \subseteq X(\omega)$. This is because $H$ fixes 1, leaves $F(\omega)$ invariant, is a subgroup of $\text{Aut}(\Gamma)$, and is transitive on $x^H$. In other words, there exists a path from 1 to every vertex of $X(\omega)$. Therefore, $\Gamma - F(\omega)$ is connected and so $F(\omega)$ is not a vertex-cut of $\Gamma$.

3.2 Proof of Theorem 3.1

Throughout this subsection we assume that $p, q, e, r$ and $h$ are as in Theorem 3.1 and residue classes are mod $q$. Define

$$H_{q,r} = \langle [h] \rangle, \text{ where } h = (p - 1)^r.$$  \hspace{1cm} (5)

Since $\gcd(h, p) = 1$, $H_{q,r}$ is a subgroup of $\mathbb{Z}_q^*$.

Denote by $\text{ord}_p(n)$ the exponent of $p$ in the canonical prime factorisation of $n$. In particular, $\text{ord}_p(n) = 0$ if $p$ is not a divisor of $n$. In the special case when $p = 3$, equality (6) below was observed in [28, Lemma 4.2].

Lemma 3.3. Let $k$ and $s$ be integers with $k \geq 0$ and $1 \leq s \leq p - 1$.

(a) If $s$ is even, then

$$\text{ord}_p((p - 1)^{ps} - 1) = k + 1.$$  \hspace{1cm} (6)

(b) If $s$ is odd, then

$$\text{ord}_p((p - 1)^{ps} + 1) = k + 1.$$  \hspace{1cm} (7)

Proof. Denote $a_{k,s} = (p - 1)^{ps}$. It is obvious that (6) and (7) are true when $k = 0$. Assume $k \geq 1$ in the sequel. We have

$$a_{1,s} = \sum_{j=0}^{ps} \binom{ps}{j} (-1)^j p^{js}.$$  \hspace{1cm} (8)
(a) Suppose that $s$ is even. Then the last term on the right-hand side of \((5)\) is 1, the second last one is $-p^2s$, and all other terms are divisible by $p^3$. Since $2 \leq s \leq p - 1$, it follows that $\text{ord}_p(a_{1,s} - 1) = 2$ and so (6) holds when $k = 1$.

Assume inductively that $\text{ord}_p(a_{k,s} - 1) = k + 1$ for some $k \geq 1$ and every even $s$ with $2 \leq s \leq p - 1$. Since for every $i \geq 0$, $p^k s i$ is even (as $s$ is even), we have $a_{k,s}^i = \sum_{j=0}^{p^k s i} (-1)^i j \equiv \sum_{j=0}^{p^k s i - 1} \equiv 1 \pmod{p^2}$. Thus $\text{ord}_p \left( \sum_{i=0}^{p-1} a_{k,s}^i \right) = 1$. Since $a_{k+1,s} - 1 = (a_{k,s} - 1) \cdot \sum_{i=0}^{p-1} a_{k,s}^i$, it follows that $\text{ord}_p(a_{k+1,s} - 1) = \text{ord}_p(a_{k,s} - 1) + \text{ord}_p \left( \sum_{i=0}^{p-1} a_{k,s}^i \right) = k + 2$, and the proof is complete by induction.

(b) Suppose that $s$ is odd. As in (a), we see from (5) that $\text{ord}_p(a_{1,s} + 1) = 2$.

Assume inductively that $\text{ord}_p(a_{k,s} + 1) = k + 1$ for some $k \geq 1$ and every odd $s$ with $1 \leq s \leq p - 2$. Similar to (a), for every $i \geq 0$, we have $a_{k,s}^i \equiv (-1)^i \pmod{p^2}$ and thus $\text{ord}_p \left( \sum_{i=0}^{p-1} (-1)^i a_{k,s}^i \right) = 1$. Since $p$ is odd, $a_{k+1,s} + 1 = a_{k,s}^p + 1 = (a_{k,s} + 1) \cdot \sum_{i=0}^{p-1} (-1)^i a_{k,s}^i$. It follows that $\text{ord}_p(a_{k+1,s} + 1) = \text{ord}_p(a_{k,s} + 1) + \text{ord}_p \left( \sum_{i=0}^{p-1} (-1)^i a_{k,s}^i \right) = k + 2$, and the proof is complete.

\section*{Lemma 3.4}

The following hold:

(a) the order of $[p - 1]$ in the multiplicative group $\mathbb{Z}^*_p$ is equal to $2p^{e-1}$;

(b) $|H_{q,r}| = 2p^{e-r-1}$, and moreover

\[ -H_{q,r} = H_{q,r} = \{ [h^i] : 0 \leq i \leq 2p^{e-r-1} - 1 \} \]

(9)

\[ \{ [p^{r+1}k \pm 1] : 0 \leq k \leq p^{e-r-1} - 1 \}. \]

(10)

\textbf{Proof.} (a) Let $d$ denote the order of $[p - 1]$ in $\mathbb{Z}^*_p$. Then $d$ is a divisor of $|\mathbb{Z}^*_p| = (p - 1)p^{e-1}$. Since $(p - 1)^d \equiv 1 \pmod{d}$, we have $(p - 1)^d \equiv 1 \pmod{d}$. On the other hand, $p - 1 \equiv -1 \pmod{d}$ implies $(p - 1)^d \equiv (-1)^d \pmod{d}$. Thus $d$ must be even and so $d = p^k s$ for some integer $k$ with $1 \leq k \leq e - 1$ and even integer $s$ dividing $p - 1$. (We have $k \geq 1$ since $(p - 1)^s \equiv 1 \pmod{q}$ when $s$ is even.) This together with (6) implies $k + 1 \geq e$. Hence $k = e - 1$ and $d = p^{e-1}s$. On the other hand, by (6), we have $(p - 1)^{2p^{e-1}} \equiv 1 \pmod{q}$. Therefore, $d = 2p^{e-1}$.

(b) Since $[p - 1]$ has order $2p^{e-1}$ in $\mathbb{Z}^*_p$, the order of $[h]$ in $\mathbb{Z}^*_q$ is $2p^{e-r-1}$. That is, $|H_{q,r}| = 2p^{e-r-1}$. Since $r \geq 0$, by (7) we have $(p - 1)(p^{e+r-1} + 1) \equiv 0 \pmod{q}$. Thus, for every $i$,

\[ (p - 1)^{p^r i} + (p - 1)^{p^r (i + p^{e-1})} = (p - 1)^{p^r i} (p - 1)^{p^{e+r-1} + 1} \equiv 0 \pmod{q}. \]

In other words, $[h^i] = -[h^{i + p^{e-1}}]$, and therefore $-H_{q,r} = H_{q,r}$.

The equality (9) holds because, by (a), $(p - 1)^{p^r (j - 1)} \equiv 1 \pmod{q}$ for $0 \leq i < j \leq 2p^{e-r-1} - 1$. By (7), we have $(p - 1)^{p^r} \equiv -1 \pmod{p^{r+1}}$ and so $(p - 1)^{p^r i} \equiv (-1)^i \pmod{p^{r+1}}$. In other words, each $[h^i] = [p^{r+1}k + (-1)^i]$ for some integer $k$. In $\mathbb{Z}_q$, there are exactly $2p^{e-r-1}$ integers of the form $p^{r+1}k \pm 1$, and for distinct $k$ between 0 and $p^{e-r-1} - 1$, these integers are different in $\mathbb{Z}_q$. Therefore, $H_{q,r} = \{ [p^{r+1}k \pm 1] : k \in \mathbb{Z} \} = \{ [p^{r+1}k \pm 1] : 0 \leq k \leq p^{e-r-1} - 1 \}$. \qed
Lemma 3.5. The set of fixed points of \([h]\) is given by

\[ F = F(h) = \{ [px] \neq [0] : x \in \mathbb{Z} \}. \tag{11} \]

Proof. Suppose that \([y] \in F(h)\). Then by (9) there exists an \(i, 1 \leq i < 2p^{e-r-1}\), such that

\[ [h^i][y] = [y], \quad \text{that is,} \quad ((p-1)^{epi} - 1) \equiv 0 \mod q. \]

Since \(0 < p^r \cdot i < 2p^{e-1}\), by part (a) of Lemma 3.3, we have \(\text{ord}_{p} \cdot ((p-1)^{epi} - 1) < e\). This together with \(((p-1)^{epi} - 1) \equiv 0 \mod q\) implies that \(p\) divides \(y\) and therefore \(F(h) \subseteq \{ [px] \neq [0] : x \in \mathbb{Z} \} = \{ [px] \in \mathbb{Z}_q : 1 \leq x \leq p^{r-1} - 1 \} \).

Conversely, consider \([px]\) with \(1 \leq x < p^{r-1} - 1\). By (9), \(p^{r-1}\) divides \((p-1)^{2r-2} - 1\). Thus \([h^{2p^{e-r-2}}][px] = (p-1)^{2p^{e-2}}[px] = [px]\) and so \([px] \in F(h)\). Therefore, \(\{ [px] \in \mathbb{Z}_q : 1 \leq x \leq p^{r-1} - 1 \} \subseteq F(h)\).

Equivalently, (11) asserts that \(X(h) \setminus \{ [0] \} = \mathbb{Z}_q^*\) (as sets). Hence \(|X(h) \setminus \{ [0] \}| = p^{r-1}(p-1)\).

Since \(|H_{q,r}| = 2p^{e-r-1}\), it follows from Lemma 3.2(b) that \(X(h) \setminus \{ [0] \}\) is the union of \(p^r(1-2) H_{q,r}\)-orbits on \(\mathbb{Z}_q \setminus \{ [0] \}\).

Proof of Theorem 3.7. Since \(-H_{q,r} = H_{q,r}\) (by Lemma 3.4(b)) and \([1] \in H_{q,r}, \Gamma_{q,r}\) is an undirected connected circulant graph. Obviously, \(\Gamma_{q,r}\) has valency \(|H_{q,r}| = 2p^{e-r-1}\) and admits \([h]\) (defined in (5)) as a complete rotation. We saw already that the set of fixed points \(F\) of \(h\) is given by (11) as claimed. Using this and the definition of \(\Gamma_{q,r}\), one can see that \(F\) is an independent set of \(\Gamma_{q,r}\).

We now prove that, if \(r \geq 1\), then \(F\) is a vertex-cut of \(\Gamma_{q,r}\). We achieve this by showing that any path in \(\Gamma_{q,r}\) from \([0]\) to \([p+1]\) must use at least one vertex of \(F\). (Note that both \([0]\) and \([p+1]\) are outside \(F\).) Suppose to the contrary that there exists a path

\[ P : [0], [h^{i_1}], [h^{i_1} + h^{i_2}], \ldots, [h^{i_1} + \cdots + h^{i_m}] = [p+1] \]

of \(\Gamma_{q,r}\) whose vertices are all in \(X(h)\). As noted in the proof of Lemma 3.4, each \([h^{i_1}] = [p^{r+1}k_i + (-1)^{i_1}]\) for some integer \(k_i\). So for any \(l\) with \(1 \leq l \leq m\), the \((l+1)\)-th vertex of \(P\) is \([p^{r+1}k_l + a_l]\), where \(k_l = \sum_{i=1}^{l} k_i\), and \(a_l = \sum_{i=1}^{l} (-1)^{i_1}\). Since all these vertices are in \(X(h)\) and are different from \([0]\) (as \(P\) is a path and so has no repeated vertices), by (11) we have \(a_l \neq 0\), \(1 \leq l \leq m\). Moreover, we can prove by induction that \((-p-1) \leq a_l \leq p-1\) for each \(l\). In fact, this is obviously true when \(l = 1\). Assume that it is true for some \(l\) with \(1 \leq l < m\). Note that \(a_{l+1} = a_l + 1\) or \(a_l - 1\). In the former case, we have \(a_l < p-1\) for otherwise \(a_{l+1} = 0\), and \([p^{r+1}k_{l+1} + a_{l+1}] = [p^{r+1}k_{l+1}] \in F\), a contradiction. Hence \((-p-1) \leq a_{l+1} \leq p-1\).

Similarly, one can see that the same inequalities hold when \(a_{l+1} = a_l - 1\). Therefore, we have proved \((-p-1) \leq a_l \leq p-1\) for \(1 \leq l \leq m\). Since the last vertex of \(P\) is \([p+1]\), we have \([p^{r+1}k_m + a_m] = [p+1]\). Thus \(a_{m-1}\) is a multiple of \(p\). This together with \((-p-1) \leq a_{m} \leq p-1\) implies that \(a_{m} = 1\) or \((-p-1)\). If \(a_{m} = 1\), then \([p^{r+1}k_m] = [p]\) and so \(p^{r+1}\) divides \(p\), which is a contradiction as \(r \geq 1\). If \(a_{m} = (-p-1)\), then \([p^{r+1}k_m - p] = [p]\) and so \(p^{r+1}\) divides \(2p\), which again is impossible as \(r \geq 1\). Therefore, we have proved that every path in \(\Gamma_{q,r}\) from \([0]\) to \([p+1]\) uses at least one vertex of \(F\). Consequently, \(F\) is a vertex-cut of \(\Gamma_{q,r}\) when \(r \geq 1\).

Finally, we prove that \(F\) is not a vertex-cut of \(\Gamma_{q,r}\) when \(r = 0\). Since \(H_{q,0} = \{ [pk \pm 1] : 0 \leq k \leq p^{r-1} - 1 \}\) by (10), one can verify that for \(1 \leq i < j \leq (p-1)/2\), \(H_{q,0} [i] \neq H_{q,0} [j]\). Since these \(H_{q,0}\)-orbits are clearly disjoint from \(F\), they must be contained in \(X(h)\). Since \(X(h) \setminus \{ [0] \}\) consists of precisely \((p-1)/2\) \(H_{q,0}\)-orbits, we conclude that \(X(h) \setminus \{ [0] \}\) is equal to the union of \(H_{q,0} [i], 1 \leq i \leq (p-1)/2\). For each \(i\) between 1 and \((p-1)/2\), there exists a path of \(\Gamma_{q,0} - F\)
from $[0]$ to at least one vertex of $H_{q,0}[i]$, say, the path $[0],[1],[2],\ldots,[i]$. By Lemma 3.2(d) we conclude that $F$ is not a vertex-cut of $\Gamma_{q,0}$.

**Acknowledgements** We thank J. Širáň for his help on regular Cayley maps and the anonymous referees for their helpful comments. The second author was supported by a Future Fellowship (FT110100629) of the Australian Research Council.

**References**

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

[2] B. Albader, B. Bose and M. Flahive, Efficient communication algorithms in hexagonal mesh interconnection networks, *IEEE Trans. Parallel and Distributed Systems* **23** (2012), 69–77.

[3] F. Annexstein, M. Baumslag and A. Rosenberg, Group action graphs and parallel architectures, *SIAM J. Comput.* **19** (1990), no. 3, 544–569.

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

[5] J.-C. Bermond, T. Kodate and S. Péroennes, 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.

[6] N. L. Biggs, *Algebraic Graph Theory*, second edition, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1993.

[7] J. A. Bondy and U. S. R. Murty, *Graph Theory*, Springer, New York, 2008.

[8] D. Bressoud and S. Wagon, *A Course in Computational Number Theory*, Key College Publishing, Emeryville, CA, 2000.

[9] C. Y. Chao, On the classification of symmetric graphs with a prime number of vertices, *Trans. Amer. Math. Soc.* **158** (1971), 247–256.

[10] M.-S. Chen, K. G. Shin and D. D. Kandlur, Addressing, routing, and broadcasting in hexagonal mesh multiprocessors, *IEEE Trans. Computers* **39** (1) (1990), 10–18.

[11] G. Cooperman and L. Finkelstein, New methods for using Cayley graphs in interconnection networks, *Discrete Appl. Math.* **37-38** (1992), 95–118.

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

[13] E. Dobson and J. Morris, Toida’s conjecture is true, *Electron. J. Combin.* **9** (1) (2002), Research Paper 35, 14 pp.

[14] J. W. Dolter, P. Ramanathan and K. G. Shin, Performance analysis of virtual cut-through switching in HARTS: a hexagonal mesh multicomputer, *IEEE Trans. Computers*, **40** (6) (1991), 669–680.

[15] P. Fragopoulou and S. G. Akl, Spanning subgraphs with applications to communication on a subclass of the Cayley-graph-based networks, *Discrete Applied Math.* **83** (1998), 79–96.

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

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

[18] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (3) (1981), 243–256.

[19] 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.

[20] M. C. Heydemann, J. C. Meyer and D. Sotteau, On forwarding indices of networks, *Discrete Applied Math.* **23** (1989), 103–123.
[21] M. C. Heydemann, N. Marlin and S. Pérennes, Complete rotations in Cayley graphs, *Europ. J. Combin.* **22** (2001), 179–196.

[22] J. Hromkovič, R. Klasing, A. Pelc, P. Ružička and W. Unger, *Dissemination of Information in Communication Networks* (broadcasting, gossiping, leader election, and fault-tolerance), Texts in Theoretical Computer Science, An EATCS Series, Springer-Verlag, Berlin, 2005.

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

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

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

[26] R. Jajcay and J. Širáň, Skew-morphism of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179.

[27] S. Lakshmivarahan, J. S. Jwo and S. K. Dhall, Symmetry in interconnection networks based on Cayley graphs of permutation groups: a survey, *Parallel Comput.* **19** (1993), no. 4, 361–407.

[28] N. Lichiardopol, Concerning two conjectures on the set of fixed points of a complete rotation of a Cayley digraph, *Discrete Math.* **280** (2004), 119–131.

[29] T. K. Lim and C. E. Praeger, Finding optimal routings in Hamming graphs, *Europ. J. Combin.* **23** (2002), 1033–1041.

[30] M. Muzychuk, M. Klin and R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, *Codes and Association Schemes* (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Vol. 56, pp.241–264, Amer. Math. Soc., Providence, RI, 2001.

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

[32] M. Škoviera and J. Širáň, Regular maps from Cayley graphs, Part I: balanced Cayley maps, *Discrete Math.* **109** (1992), 265–276.

[33] P. Solé, The edge-forwarding index of orbital regular graphs, *Discrete Math.* **130** (1994), no. 1-3, 171–176.

[34] A. Thomson and S. Zhou, Gossiping and routing in undirected triple-loop networks, *Networks* **55** (4) (2010), 341–349.

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

[36] A. Thomson and S. Zhou, Frobenius circulant graphs of valency six, Eisenstein-Jacobi networks, and hexagonal meshes, *Europ. J. Combin.*, to appear.

[37] C. K. Wong and D. Coppersmith, A combinatorial problem related to multmodule memory organizations, *J. ACM* **21** (1974), 392–402.

[38] 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.

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

[40] S. Zhou, On 4-valent Frobenius circulant graphs, *Disc. Math. and Theoretical Comp. Sci.* **14** (2) (2012), 173–188.