A class of arc-transitive Cayley graphs as models for interconnection networks

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

June 10, 2008

Abstract

We study a class of Cayley graphs as models for interconnection networks. With focus on efficient communication we prove that for any graph in the class there exists a gossiping protocol which exhibits attractive features, and moreover we give an algorithm for constructing such a protocol. In particular, these hold for two important subclasses of graphs, namely, Cayley graphs admitting a complete rotation and Frobenius graphs of a certain type. For such Frobenius graphs, we obtain the minimum gossip time and give an optimal gossiping protocol under which messages are transmitted along shortest paths and each arc is used exactly once at each time step. Moreover, for such Frobenius graphs we construct an all-to-all routing which is a shortest path routing, arc-transitive, edge- and arc-uniform, and optimal for the edge- and arc-forwarding indices simultaneously.

Key words: Cayley graph; arc-transitive graph; orbital-regular graphs; Frobenius group; Frobenius graph; complete rotation; communication algorithm; interconnection network; gossiping; minimum gossip time; edge-forwarding index; arc-forwarding index

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

1 Introduction

An interconnection network is often modelled by an undirected graph in which vertices represent processors, memory modules or routers, and edges represent bidirectional communication links. To achieve high performance mathematicians and computer scientists recommend (e.g. [1, 18, 23]) Cayley graphs as models for interconnection networks because of the many advantages [18] that they exhibit. In fact, a number of networks of both theoretical and practical importance, including hypercubes, butterflies, cube-connected cycles, star graphs and their generalisations, are Cayley graphs. The reader is referred to the survey papers [18, 23] for a large number of results pertaining to Cayley graphs as models for interconnection networks.

Given a group G and a subset $S \subseteq G \setminus \{1\}$ such that $S = S^{-1} := \{s^{-1} : s \in S\}$ (where 1 is the identity element of G), the *Cayley graph* on G relative to S, denoted by $\mathrm{Cay}(G, S)$, is defined to have vertex set G and edge set $\{\{x, y\} : x, y \in G, xy^{-1} \in S\}$. Obviously, the class of Cayley graphs is huge, and thus the following problem arises naturally: which Cayley graphs should we use for the purpose of constructing high performance interconnection networks? This general

*Supported by a Discovery Project Grant of the Australian Research Council and an Early Career Researcher Grant of The University of Melbourne.

problem has been investigated extensively from different angles, and a number of Cayley graphs have been proposed and studied; see e.g. [1, 3, 7, 10, 25, 26, 28]. Of course the answer to this problem depends on the measures of performance that we are concerned with. In this paper we will focus on efficiency of communication, which is typically measured by certain invariants such as the vertex-forward index [6], edge-forwarding index [20], minimum gossip time [4], etc. In this regard researchers have published a large number of papers on various information dissemination problems; see for example [21] for a survey on broadcasting and gossiping. In particular, much attention has been paid to finding Cayley networks with desirable routing protocols. In this direction Heydemann, Meyer and Sotteaut [20] proved that any Cayley graph admits an all-to-all routing of shortest paths with uniform load on all vertices. It was observed [18] that similar statement for edges is not true in general. However, Solé [30] proved that for a certain family of graphs, called *orbital-regular graphs*, there exists an all-to-all routing of shortest paths such that the load on all edges is uniform. In [11], Fang, Li and Praeger proved that a graph is orbital-regular if and only if it is a cycle C_n, a star $K_{1,n-1}$, or a Frobenius graph whose definition will be given in Section 2.

In 1995, Bermond, Kodate and Pérennes [4] introduced the concept of complete rotation in a Cayley graph $\mathrm{Cay}(G, S)$, which can be defined as an automorphism of G that induces a cyclic permutation on S. Under the full-duplex all-port communication model, they provided an optimal gossip algorithm for any Cayley graph which admits a complete rotation and satisfies a certain condition. Independently, Fragopoulou, Akl and Meijer [12, 13, 14] introduced a similar but more restrictive concept of rotation in Cayley graphs, which turns out to be a complete rotation induced by an inner automorphism of the underlying group. In [13] Fragopoulou and Akl explicitly gave such rotations for hypercubes, multidimensional tori, star graphs, bubble sort graphs and a few other popular Cayley graphs. For an arbitrary Cayley graph admitting such a rotation, Fragopoulou and Akl [13] constructed certain spanning subgraphs which enable near-optimal routings for three communication problems. In [19] Heydemann, Marlin and Pérennes investigated Cayley graphs admitting a complete rotation and gave an account of known results on such graphs. Examples of rotational Cayley graphs include Hamming graphs $H(d, q)$, that is, Cartesian product of d copies of the complete graph K_q, where q is a prime power. In [24], Lim and Praeger proved that $H(d, q)$ is an orbital-regular graph if and only if each prime divisor of d divides $q - 1$.

Inspired by the researches above, in this paper we expand the notions of complete rotation and orbital-regularity and study the class of Cayley graphs $\mathrm{Cay}(G, S)$ such that the setwise stabiliser of S in $\mathrm{Aut}(G)$, $\mathrm{Aut}(G, S)$, contains a subgroup which acts regularly on S. This class contains all Cayley graphs admitting a complete rotation and all Frobenius graphs of the first type (see Section 2 for definition). We prove that for any graph in this class there exists a gossiping protocol which exhibits very attractive features essential for efficient communication, and moreover we give an algorithm for constructing such a protocol. (See Theorem 4.1, Algorithm 4.3 and Corollary 4.4 for details.) In particular, for Frobenius graphs of the first type we find simple formulae for the minimum gossip time, the edge-forwarding index and the arc-forwarding index, and give explicitly an all-to-all routing which is (i) a shortest path routing, (ii) arc-transitive, (iii) both edge- and arc-uniform, and (iv) optimal for these invariants simultaneously. (See Theorems 5.1 and 6.1. A generalisation of Theorem 5.1 is given in Theorem 5.3.) Moreover, the work in this paper extends the framework in [13, Section 4] to a much larger class of Cayley graphs and answers the question in [13, lines 13-15, Section 6].

The rest of this paper is organised as follows. In the next section we will introduce the notation and terminology that will be used throughout. As demonstrated in [13] and many other papers, a gossiping protocol can be induced by a family of spanning subgraphs of the underlying network. In Section 3 we will prove the existence of a certain family of spanning subgraphs of any Cayley graph $\mathrm{Cay}(G, S)$ such that $\mathrm{Aut}(G, S)$ contains a subgroup H acting transitively on S (Theorem 3.1). Such spanning subgraphs play a fundamental role in our subsequent discussion on gossiping and routing. In Section 4 we will give a gossiping protocol (Algorithm 4.3) for Cayley graphs $\mathrm{Cay}(G, S)$ with H regular on S, and summarize main features of this protocol in Theorem 4.1 and Corollary 4.4. In Sections 5 and 6 we will discuss the minimum gossip time and the edge- and arc-forwarding indices of Frobenius graphs of the first type, respectively. The paper ends with examples and remarks.

2 Preliminaries

We will consider only finite groups and use standard notation and terminology (see e.g. [9]) on permutation groups. For a set V and a group G with identity 1, 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 $g, h \in G$. As usual 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 *stabiliser* of v in G. The group G is said to be *semiregular* on V if $G_v = 1$ 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. For $U \subseteq V$, denote $U^g := \{u^g : u \in U\}$ and let $G_U := \{g \in G : U^g = U\}$ be the *setwise stabiliser* of U in G. For two groups K, H, if H acts on K (as a set) such that $(xy)^h = x^h y^h$ for any $x, y \in K$ and $h \in H$, then H is said to act on K as a group. In this case we use $K : H$ to denote the *semidirected product* [9, 27] of K by H with respect to the action.

For a graph $\Gamma = (V(\Gamma), E(\Gamma))$, denote by $\mathtt{Arc}(\Gamma)$ the set of arcs of Γ, where an *arc* is an ordered pair of adjacent vertices. For $x, y \in V(\Gamma)$, $d(x, y)$ denotes the distance in Γ between x and y, and d the diameter of Γ. For $i = 0, 1, \dots, d$, define

$$\Gamma_i(x) := \{y \in V(\Gamma) : d(x, y) = i\}.$$

In particular, $\Gamma(x) := \Gamma_1(x)$ is the *neighbourhood* of x in Γ. Let G be a group of automorphisms of Γ, that is, G acts on $V(\Gamma)$ and preserves the adjacency of Γ. Then G induces an action on $\mathtt{Arc}(\Gamma)$ defined by $(x, y)^g := (x^g, y^g)$, where $g \in G$ and $(x, y) \in \mathtt{Arc}(\Gamma)$. In the case when G is transitive on $\mathtt{Arc}(\Gamma)$, Γ is called a *G-arc transitive graph.*

From now on we will use $\Gamma = \mathrm{Cay}(G, S)$ *to denote a Cayley graph with degree* $\delta := |S|$ *and diameter* d*, and we assume that* Γ *is connected, that is,* $\langle S \rangle = G$. The identity element of G will be denoted by 1 throughout. The arcs of Γ will be thought as coloured by the elements of S: for $x, y \in G$ adjacent in Γ, the arcs (x, y), (y, x) receive *colours* xy^{-1}, yx^{-1}, respectively. It is well-known that $G \times G \to G$, $(x, g) \mapsto xg$, $x, g \in G$, defines a regular action of G on G (as a set). The permutation $x \mapsto xg$, $x \in G$, induced by g is called a *translation*. Under this translation the image of a subset X of G is $Xg := \{xg : x \in X\}$. This regular action of G on G preserves the adjacency of Γ (see e.g. [5]), and hence we may take G as a subgroup of the automorphism group $\mathrm{Aut}(\Gamma)$ of Γ. Let

$$\mathrm{Aut}(G, S) := \mathrm{Aut}(G)_S = \{\phi \in \mathrm{Aut}(G) : S^\phi = S\}$$

be the setwise stabiliser of S in $\mathrm{Aut}(G)$ under the natural action of $\mathrm{Aut}(G)$ on G. (In [19] $\mathrm{Aut}(G,S)$ is denoted by $\mathrm{Stab}(G,S)$ and an element of $\mathrm{Aut}(G,S)$ is called an S-*stabliser* of G.) Of course, $\mathrm{Aut}(G,S)$ is a subgroup of $\mathrm{Aut}(G)$. Moreover, regarded as a permutation of the vertices of Γ, each element of $\mathrm{Aut}(G,S)$ is a graph automorphism of Γ which fixes the vertex 1 [5, Proposition 16.2]. Hence

$$\mathrm{Aut}(G,S) \le \mathrm{Aut}(\Gamma)_1 \le \mathrm{Aut}(\Gamma), \tag{1}$$

where $\mathrm{Aut}(\Gamma)_1$ is the stabiliser of 1 in $\mathrm{Aut}(\Gamma)$. In [16, Lemma 2.1] it was proved that the normalizer of G in $\mathrm{Aut}(\Gamma)$ is $G : \mathrm{Aut}(G,S)$. Since $G : \mathrm{Aut}(G,S)$ is a subgroup of the holomorph $\mathrm{Hol}(G)$ [27] of G, it acts on G in the same way as $\mathrm{Hol}(G)$ acts on G. See Figure 1 for relationships among the groups in this paragraph.

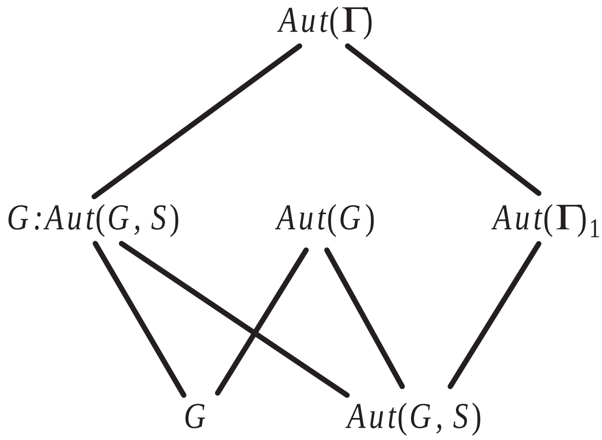

Figure 1: Relationships among the groups in this section.

The following observation will be used in our subsequent discussion. Since G is a normal subgroup of $G : \mathrm{Aut}(G,S)$, the elements of $G : \mathrm{Aut}(G,S)$ have the form ϕg, $\phi \in \mathrm{Aut}(G,S)$, $g \in G$.

Lemma 2.1 *Let $\Gamma = \mathrm{Cay}(G,S)$ be a connected Cayley graph over a finite group G. Let $H \le \mathrm{Aut}(G,S)$. Then Γ is $G : H$-arc transitive if and only if H is transitive on S, that is, S is an H-orbit on G.*

Proof Let (x,y) and (u,v) be arcs of Γ. Then $x = ay$ and $u = bv$ for some $a,b \in S$ by the definition of Γ. Suppose that H is transitive on S. Then there exists $\phi \in H$ such that $a^\phi = b$. Let $g = (y^\phi)^{-1}v$. Then $y^{\phi g} = (y^\phi)^g = y^\phi g = v$, and hence $x^{\phi g} = (ay)^{\phi g} = ((ay)^\phi)^g = (a^\phi y^\phi)g = by^\phi g = bv = u$. Thus, $(x,y)^{\phi g} = (u,v)$ and $G : H$ is transitive on $\mathtt{Arc}(\Gamma)$.

Suppose conversely that Γ is $G : H$-arc transitive. For any $a,b \in S$, since $(a,1)$ and $(b,1)$ are arcs of Γ, there exists $\phi g \in G : H$ (where $g \in G$ and $\phi \in H$) such that $(b,1) = (a,1)^{\phi g}$. Thus, $1 = 1^{\phi g} = g$ and $b = a^{\phi g} = a^\phi g = a^\phi$, and hence H is transitive on S. □

A *Frobenius group* is a transitive permutation group L on a set V which is not regular on V, but has the property that the only element of L which fixes two points of V is the identity of L. It is well-known (see e.g. [9, pp.86]) that a finite Frobenius group L has a nilpotent normal subgroup G, called the *Frobenius kernel*, which is regular on V. Hence L is the semidirect product $G : H$, where H is the stabiliser of a point of V; each such group H is called a *Frobenius complement* of G in L. Given a Frobenius group $L = G : H$, an *L-Frobenius graph* [11] is a connected graph with vertex set V and edge set $\{\{x, y\} : (x, y) \in O\}$ for some L-orbital O in $\{(x, y) : x, y \in V, x \neq y\}$. Since G is regular on V, we may identify V with G in such a way that G acts on itself by right multiplication, and we may take H as the stabiliser of 1 (identity of G) such that H acts on G by conjugation. In the following we will adopt this convention. It was proved in [11, Theorem 1.4] that any L-Frobenius graph is a Cayley graph $\mathrm{Cay}(G, S)$ on its Frobenius kernel G, where

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

for some $a \in G$ satisfying $\langle a^H \rangle = G$, where $|a|$ is the order of a. Here, for $x \in G$, $x^H := \{h^{-1}xh : h \in H\}$ is the H-orbit containing x under the action of H on G (by conjugation). Conversely, for any $a \in G$ with $\langle a^H \rangle = G$, the Cayley graph $\mathrm{Cay}(G, S)$ with respect to the above-defined S is an L-Frobenius graph. Since L is a Frobenius group, we may take H as a subgroup of $\mathrm{Aut}(G)$ so that $H \leq \mathrm{Aut}(G, S)$. Moreover, H is semiregular on $G \setminus \{1\}$. We call $\mathrm{Cay}(G, S)$ an L-Frobenius graph of the *first (second) type* if S is given in the first (second) line of (2). Note that, if $\mathrm{Cay}(G, S)$ is of the first type, then H is regular on S.

Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley graph. A bijection $\omega : G \to G$ is called a *complete rotation* [4] of Γ if there exists an ordering of $S = \{s_0, s_1, \ldots, s_{\delta-1}\}$ such that

$$\omega(1) = 1,\ \omega(xs_i) = \omega(x)s_{i+1}$$

for all $x \in G$ and $i = 0, 1, \ldots, \delta-1$ with subscripts modulo δ. In particular, $\omega(s_i) = s_{i+1}$ for each i and so ω permutes the elements of S cyclically. As observed in [24], a complete rotation is a special case of a skew-morphism [22], and the existence of a complete rotation of Γ is equivalent to the existence of a balanced regular Cayley map [29] with Γ as the underlying graph. In [19, Proposititon 2.2] it is shown that a bijection $\phi : G \to G$ is a complete rotation of Γ if and only if $\phi \in \mathrm{Aut}(G, S)$ and ϕ induces a cyclic permutation on S, called a *cyclic S-stabliser* of G [19]. In other words, a complete rotation is an element ϕ of $\mathrm{Aut}(G, S)$ such that, for some (and hence all) $s \in S$, $s^{\langle \phi \rangle} = \{s, s^{\phi}, s^{\phi^2}, \ldots, s^{\phi^{\delta-1}}\} = S$. In [13] a *rotation* of Γ is defined to be an inner automorphism of G, say, $\phi : x \mapsto x^g := g^{-1}xg,\ x \in G$, such that $\phi \in \mathrm{Aut}(G, S)$ and ϕ induces a cyclic permutation on S. Thus, a rotation of Γ is an inner automorphism of G which is a complete rotation ϕ. It is shown [13] that some popular Cayley networks, including hypercubes, multidimensional tori, star graphs, modified bubble-sort graphs, bisectional networks, all admit rotations. See [18, Appendix] or [19, Appendix A] for details.

The objects of study in this paper are Cayley graphs $\mathrm{Cay}(G, S)$ such that $\mathrm{Aut}(G, S)$ contains a subgroup H which is regular on S. By Lemma 2.1 such a graph is $G : H$-arc transitive, justifying the title of this paper. Let $\mathbf{R}$ denote the class of such graphs, and $\mathbf{F}$ the class of Frobenius graphs of the first type. Let $\mathbf{CR}$ ($\mathbf{RO}$, respectively) denote the class of Cayley graphs admitting a complete rotation (rotation, respectively). From the previous paragraph, if $\mathrm{Cay}(G, S)$ admits a complete rotation $\phi \in \mathrm{Aut}(G, S)$, then $\langle \phi \rangle$ is regular on S and so $\mathrm{Cay}(G, S) \in \mathbf{R}$. Hence $\mathbf{RO} \subseteq \mathbf{CR} \subseteq \mathbf{R}$. Moreover, we have $\mathbf{F} \subseteq \mathbf{R}$ from the above discussion on Frobenius graphs. In fact, **F** is identical with the subclass of **R** consisting of those Cayley graphs $\mathrm{Cay}(G, S)$ such that H is regular on S and semiregular on $G \setminus \{1\}$ for some $1 \neq H \leq \mathrm{Aut}(G, S)$, because in this case $G : H$ is a Frobenius group and $\mathrm{Cay}(G, S)$ is a first type $G : H$-Frobenius graph. Note that $\mathbf{CR} \cap \mathbf{F} \neq \emptyset$ since by [24, Theorem 1.3, Section 5] any Hamming graph $H(d, q)$ with q a prime and every prime divisor of d dividing $q - 1$ belongs to both **CR** and **F**. By [13, Lemma 8], hypercubes Q_d of dimension $d \geq 3$ are members of **RO**. Since, for example, 3 is not a divisor of $2^3 - 1$, we have $Q_3 \notin \mathbf{F}$ and hence $\mathbf{CR} \setminus \mathbf{F} \neq \emptyset$. This fact also follows from the discussion in [24, Section 5].

The classes of graphs above are illustrated in Figure 2. Notation and terminology concerning communication and routing will be introduced in subsequent sections when needed.

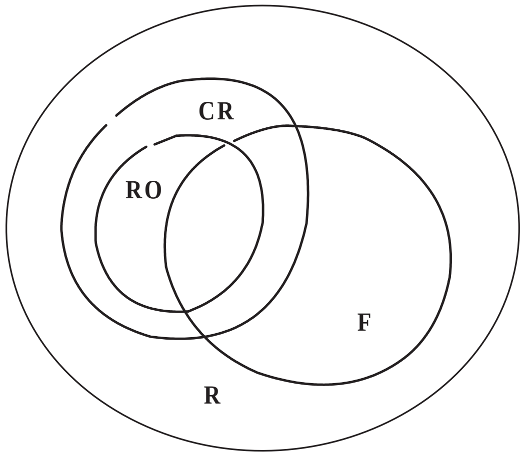

Figure 2: Classes of Cayley graphs considered and their relations. **R**: Cayley graphs $\mathrm{Cay}(G, S)$ with $\mathrm{Aut}(G, S)$ containing a subgroup regular on S; **F**: Frobenius graphs of the first type; **CR**: Cayley graphs admitting a complete rotation; **RO**: Cayley graphs admitting a rotation.

3 Spanning subgraphs

In this section we will construct a family of spanning subgraphs of any connected Cayley graph $\Gamma = \mathrm{Cay}(G, S)$ such that there exists a subgroup H of $\mathrm{Aut}(G, S)$ acting transitively on S. (Note that H is not required to be regular on S in this section.) Since H is transitive on S, Γ is $G : H$-arc transitive by Lemma 2.1. For $\psi \in \mathrm{Aut}(\Gamma)$ and a subgraph Δ of Γ, the image of Δ under ψ, denoted by Δ^ψ, is the subgraph of Γ with $V(\Delta^\psi) = \{x^\psi : x \in V(\Delta)\}$ and $E(\Delta^\psi) = \{\{x^\psi, y^\psi\} : \{x, y\} \in E(\Delta)\}$. In particular, for $g \in G \leq \mathrm{Aut}(\Gamma)$, Δ^g is the subgraph of Γ with edge set $\{\{xg, yg\} : \{x, y\} \in E(\Delta)\}$, and we say that Δ^g is obtained from Δ by *translation* g. The arcs (x^ψ, y^ψ), $\psi \in \mathrm{Aut}(\Gamma)$, are said to be in the *same position*. It can be verified that $(\Delta^\psi)^\rho = \Delta^{\psi\rho}$ for any $\psi, \rho \in \mathrm{Aut}(\Gamma)$. Thus, $\mathrm{Aut}(\Gamma)$ induces an action on the set of subgraphs of Γ under which the subgraphs in the same orbit are isomorphic to each other. It is evident that, for $\psi \in \mathrm{Aut}(\Gamma)$, Δ is a spanning subgraph of Γ if and only if Δ^ψ is a spanning subgraph of Γ. For $X \subseteq G$ and a spanning subgraph Δ of Γ, define

$$\Delta(X) := \{y \in G \setminus X : y \text{ is adjacent to at least one vertex of } X \text{ in } \Delta\}.$$

A subtree Δ of Γ is called a *shortest path subtree of* Γ *rooted at* g, where g is a fixed vertex of Δ, if for each $x \in V(\Delta)$ the unique path in Δ from g to x is a shortest path in Γ; and Δ is called a *shortest path spanning tree of* Γ *rooted at* g if in addition Δ is a spanning tree of Γ.

The following theorem will be used repeatedly in subsequent sections. In its proof the promised family of spanning subgraphs will be constructed in an inductive manner. Such a construction is the basis for the gossiping protocols and the optimal routings that will be given in Sections 4, 5 and 6, respectively. Given subgraphs $\Gamma_1, \ldots, \Gamma_k$ of Γ, denote by $\bigcup_{i=1}^k \Gamma_i$ the *union* of them, that is, the subgraph of Γ with vertex set $\bigcup_{i=1}^k V(\Gamma_i)$ and edge set $\bigcup_{i=1}^k E(\Gamma_i)$.

Theorem 3.1 *Let* $\Gamma = \mathrm{Cay}(G,S)$ *be a connected Cayley graph of degree* $\delta = |S|$ *and diameter* d*. Suppose that there exists a subgroup* H *of* $\mathrm{Aut}(G,S)$ *which is transitive on* S*. Then there exists a family* $\mathcal{A} := \{\Delta_g : g \in G\}$ *of connected spanning subgraphs of* Γ *with* Δ_g *rooted at* g *such that the following hold, where in (b)-(d)* g *is an arbitrary element of* G*.*

(a) G *is transitive on* $\mathcal{A}$*; more explicitly,* $\Delta_g = \Delta_1^g$ *for any* $g \in G$ *and thus* Δ_g $(g \in G)$ *are isomorphic to each other via translations;*

(b) $\Delta_g = \bigcup_{\phi \in H} \Delta_{g,\phi}$, $\Delta_{g,\phi} = (\Delta_{1,1})^{\phi g}$ $(\phi \in H)$*,* $\Delta_{g,\phi}$ *is a shortest path subtree of* Γ *rooted at* g *and with* g *as a degree-one vertex, and each edge of* Δ_g *joins a vertex in* $\Gamma_i(g)$ *to a vertex in* $\Gamma_{i+1}(g)$ *for some* i, $0 \le i \le d-1$*;*

(c) $g^{-1}Hg$ *is transitive on* $\{\Delta_{g,\phi} : \phi \in H\}$*, and thus the subtrees* $\Delta_{g,\phi}$ $(\phi \in H)$ *of* Δ_g *are isomorphic to each other; moreover, each* $\Delta_{g,\phi}$ *contains exactly one vertex from each* $g^{-1}Hg$*-orbit on* G*, and each element of* S *is used exactly* $|H|/\delta$ *times (counting possible multiplicity) as colours by those arcs of* $\Delta_{g,\phi}$ $(\phi \in H)$ *which are in the same position;*

(d) *each vertex* $x \in G$ *of* Γ *lies in exactly* $|H_x|$ *subtrees* $\Delta_{g,\phi}$ $(\phi \in H)$ *of* Δ_g*, and* Δ_g *contains at least* $|H_x|$ *shortest paths of* Γ *from* g *to* x*; moreover, for any edge* $\{x, v\}$ *of* Δ_g*, where* $x \in \Gamma_{i+1}(g)$ *and* $v \in \Gamma_i(g)$ *for some* i*, we have* $\Delta_g(x^H) \cap \Gamma_i(g) = v^H$*.*

Moreover, Δ_g *is a shortest path spanning tree of* Γ *if and only if* $G : H$ *is a Frobenius group with Frobenius kernel* G*, where* H *is a Frobenius complement of* G*, and in this case* Γ *is a* $G : H$*-Frobenius graph of the first type.*

Proof Since H leaves S invariant and is transitive on S, S is an H-orbit on G and hence $S = s^H$ for any $s \in S$. We will first construct Δ_g for $g = 1$, and then obtain Δ_g from Δ_1 for any $g \in G$ via translations. Since $H \le \mathrm{Aut}(\Gamma)$ and H fixes 1 by (1), we have the following:

Claim 1. For $0 \le i \le d$, $\Gamma_i(1)$ is an H-invariant subset of G; in other words, $\Gamma_i(1)$ is a union of some H-orbits on G.

Let us fix an element a of S and construct a shortest path subtree $\Delta_{1,1}$ of Γ with root 1 and containing the edge $\{1, a\}$. (Indeed a is adjacent to 1 since $a \in S$.) To this end we will construct inductively $L_i(1) := \Gamma_i(1) \cap V(\Delta_{1,1})$, the set of vertices of $\Delta_{1,1}$ with distance i from 1 in Γ, together with the edges between $L_i(1)$ and $L_{i-1}(1)$ such that the following (i)-(ii) hold:

(i) each H-orbit contained in $\Gamma_i(1)$ contains exactly one vertex of $L_i(1)$; and

(ii) each vertex of $L_i(1)$ is adjacent to exactly one vertex of $L_{i-1}(1)$ in $\Delta_{1,1}$.

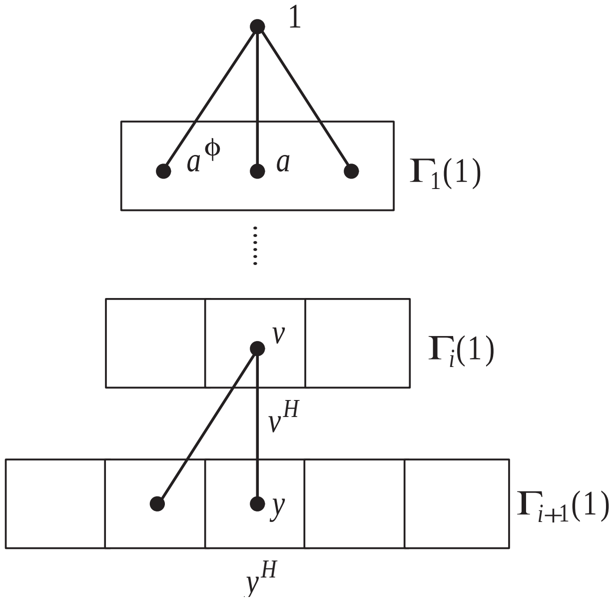

Figure 3: Proof of Theorem 3.1.

Initially, set $L_0(1) = \{1\}$, $L_1(1) = \{a\}$, and let the edge $\{1, a\}$ of Γ be in $\Delta_{1,1}$. For any H-orbit x^H contained in $\Gamma_2(1)$, since $d(1, x) = 2$, x must be adjacent to a vertex b in $\Gamma(1) = S$. Since H is transitive on S, there exists $\phi \in H$ such that $b^\phi = a$. Since ϕ is an automorphism of Γ by (1), it follows that x^ϕ is adjacent to a in Γ. Add this very vertex x^ϕ together with the edge $\{x^\phi, a\}$ to $\Delta_{1,1}$, and apply this procedure to each H-orbit x^H contained in $\Gamma_2(1)$. In this way we have constructed $L_2(1)$ such that the conditions (i)-(ii) above are satisfied for $i = 1, 2$.

Inductively, suppose that we have chosen one vertex from each H-orbit contained in $\Gamma_i(1)$ and added an edge of Γ joining it and a vertex in $\Gamma_{i-1}(1)$ to $\Delta_{1,1}$. In other words, the subgraph of $\Delta_{1,1}$ up to layer $L_i(1)$ has been constructed and (i)-(ii) are satisfied up to this layer. If $i = d$, then stop and output $\Delta_{1,1}$; otherwise we continue as follows.

Claim 2. Under the induction hypothesis above, each H-orbit x^H contained in $\Gamma_{i+1}(1)$ contains a vertex which is adjacent to at least one vertex in $L_i(1)$.

In fact, since $d(1, x) = i + 1$, there exists $u \in \Gamma_i(1)$ such that x, u are adjacent in Γ. By Claim 1, u^H is contained entirely in $\Gamma_i(1)$, and by our induction hypothesis there exists exactly one vertex $v \in u^H$ such that $v \in L_i(1)$. Now that $v \in u^H$, there exists $\phi \in H$ such that $v = u^\phi$. Let $y = x^\phi$, so that $y \in x^H$ and $y \in \Gamma_{i+1}(1)$ by Claim 1. Since x and u are adjacent and $\phi \in \mathrm{Aut}(\Gamma)$ by (1), y and v must be adjacent in Γ, and hence Claim 2 follows. See Figure 3 for an illustration.

From Claim 2 and using the notation above, we can add y together with the edge $\{y, v\}$ to $\Delta_{1,1}$, and we do this for each H-orbit x^H contained in $\Gamma_{i+1}(1)$. In this way we have constructed $L_{i+1}(1)$ together with the edges of $\Delta_{1,1}$ between $L_{i+1}(1)$ and $L_i(1)$ such that (i)-(ii) are satisfied up to layer $L_{i+1}(1)$. If $i + 1 = d$, then stop and output $\Delta_{1,1}$; otherwise set $i := i + 1$ and repeat the procedure above. Since Γ is a finite graph, we can finish the construction of $\Delta_{1,1}$ in $d + 1$ rounds. From (i)-(ii) one can check that $\Delta_{1,1}$ is a subtree of Γ rooted at 1 and the unique path between 1 and any vertex of $\Delta_{1,1}$ is a shortest path in Γ. In other words, $\Delta_{1,1}$ is a shortest path subtree of Γ with root 1. It is clear that 1 is a degree-one vertex in $\Delta_{1,1}$. Moreover, from (i) it follows that $\Delta_{1,1}$ contains exactly one vertex from each H-orbit on G.

Note that, for distinct H-orbits x^H contained in $\Gamma_{i+1}(1)$, the two vertices y guaranteed by Claim 2 may be adjacent to the same vertex v in $L_i(1)$.

For any $\phi \in H$, define

$$\Delta_{1,\phi} := (\Delta_{1,1})^{\phi}. \quad (3)$$

Since ϕ fixes 1, 1 is a vertex of $\Delta_{1,\phi}$ and so we may take 1 as the root of $\Delta_{1,\phi}$. Obviously, H is transitive on $\{\Delta_{1,\phi} : \phi \in H\}$. From the definition of $(\Delta_{1,1})^{\phi}$ it follows that $\Delta_{1,\phi}$ is isomorphic to $\Delta_{1,1}$ via the restriction of ϕ to $\Delta_{1,1}$, and moreover it contains $\{1, a^{\phi}\}$ and has 1 as a degree-one vertex. Since $\Delta_{1,1}$ is a shortest path subtree of Γ rooted at 1, so is $\Delta_{1,\phi}$. Using the notation in the proof of Claim 2, since y is the unique vertex of $\Delta_{1,1}$ in the H-orbit y^H $(= x^H)$, y^{ϕ} is the unique vertex of $\Delta_{1,\phi}$ in y^H. Since $yv^{-1} \in S$ and ϕ fixes S setwise, the arc (y^{ϕ}, v^{ϕ}) of $\Delta_{1,\phi}$ is coloured by $y^{\phi}(v^{\phi})^{-1} = (yv^{-1})^{\phi} \in S$. For $\phi, \psi \in H$, (y^{ϕ}, v^{ϕ}) and (y^{ψ}, v^{ψ}) are in the 'same position', and they receive the same colour if and only if $\phi\psi^{-1} \in H_{yv^{-1}}$. Thus, each colour is used by such arcs exactly $|H|/\delta$ times when multiplicity is taken into account. (Since $(y^{\phi}, v^{\phi}) = (y^{\psi}, v^{\psi})$ for $\phi, \psi \in (H_y)_v$, repetition arises when $(H_y)_v \neq 1$.) In particular, when H is regular on S we have $|H| = |S| = \delta$ and hence each colour from S is used exactly once by such arcs in the "same position".

Define

$$\Delta_1 := \bigcup_{\phi \in H} \Delta_{1,\phi}. \quad (4)$$

Then Δ_1 is connected since all $\Delta_{1,\phi}$ are connected and have a common vertex 1. Moreover, Claim 1 and the construction of $\Delta_{1,1}$ imply that

$$\Delta_1(y^H) \cap \Gamma_i(1) = v^H.$$

Let z be an arbitrary vertex of Γ. Without loss of generality we may assume that $z \in y^H$, where $y \in L_{i+1}(1)$ as in the proof of Claim 2. Then there exists $\phi \in H$ such that $z = y^{\phi}$, and hence $z \in \Delta_{1,\phi}$. Thus each vertex of Γ is a vertex of at least one subtree $\Delta_{1,\phi}$ with $\phi \in H$, and consequently Δ_1 is a spanning subgraph of Γ. Moreover, for any $\psi \in H$, since $z = y^{\phi} \in y^H$ and y^{ψ} is the unique vertex of $\Delta_{1,\psi}$ which is contained in y^H, we have: $z \in \Delta_{1,\psi} \Leftrightarrow z = y^{\psi}$ $\Leftrightarrow \psi\phi^{-1} \in H_y$. Therefore, each vertex in y^H belongs to exactly $|H_y| = |H|/|y^H|$ subtrees $\Delta_{1,\phi}$ $(\phi \in H)$, and hence Δ_1 contains at least $|H_y|$ shortest paths of Γ from 1 to y. In particular, noting that $S = a^H$ is an H-orbit on G, we have the following: $G : H$ is a Frobenius group with Frobenius kernel G (where H is a Frobenius complement of G) $\Leftrightarrow$ H is semiregular on $G \setminus \{1\}$ $\Leftrightarrow$ $|H_x| = 1$ for each $x \in G \setminus \{1\}$ $\Leftrightarrow$ each vertex of Γ other than 1 is in exactly one subtree $\Delta_{1,\phi}$ $\Leftrightarrow$ Δ_1 is a spanning tree of Γ rooted at 1 $\Leftrightarrow$ Δ_1 is a shortest path spanning tree of Γ. In this case since $S = S^{-1}$ there exists $\phi \in H$ such that $a^{\phi} = a^{-1}$ and so $a^{\phi^2} = a$. Hence $\phi^2 = 1$ by the semiregularity of H on $G \setminus \{1\}$. Thus, either $|a| = 2$ or $|H|$ is even, and hence Γ is a $G : H$-Frobenius graph of the first type.

Up to now we have proved that, for $g = 1$, Δ_g satisfies (b)-(d) in the theorem. For an arbitrary $g \in G$, let $\Delta_g := \Delta_1^g$ and $\Delta_{g,\phi} := (\Delta_{1,\phi})^g$ (where $\phi \in H$) be translations of Δ_1 and $\Delta_{1,\phi}$ by g respectively. Since Δ_1 is a connected spanning subgraph of Γ, so is Δ_g. Moreover, from (3) and (4) it follows that

$$\Delta_g = \bigcup_{\phi \in H} \Delta_{g,\phi}, \quad \Delta_{g,\phi} = (\Delta_{1,1})^{\phi g}. \tag{5}$$

Obviously, Δ_g is isomorphic to Δ_1, and one can verify that it inherits (b)-(d) from Δ_1. For example, since $\Delta_{g,\phi} = (\Delta_{1,1})^{\phi g} = (\Delta_{g,1})^{g^{-1}\phi g}$, $g^{-1}Hg$ is transitive on $\{\Delta_{g,\phi} : \phi \in H\}$. Using the notation in the construction of $\Delta_{1,1}$, since y is the unique vertex of $\Delta_{1,1}$ in the H-orbit y^H $(= x^H)$, $y^{\phi g}$ is the unique vertex of $\Delta_{g,\phi}$ in the $g^{-1}Hg$-orbit $(y^g)^{g^{-1}Hg} = y^H g$. That is, each $\Delta_{g,\phi}$ contains exactly one vertex from each $g^{-1}Hg$-orbit on G. Moreover, for any $x, g \in G$, we have $\Delta_g^{g^{-1}x} = (\Delta_1^g)^{g^{-1}x} = \Delta_1^x$, and hence G is transitive on $\{\Delta_g : g \in G\}$. □

Remark 3.2 (a) By (5) we have $\Delta_g = \bigcup_{\phi \in H} (\Delta_{1,1})^{\phi g}$ for $g \in G$. Thus, all Δ_g are determined by $\Delta_{1,1}$ and the action of $G : H$ on G. Note that $(\Delta_{1,1})^{\phi g}$ has vertices $x^{\phi} g$ with x running over all vertices of $\Delta_{1,1}$, and edges $\{x^{\phi} g, w^{\phi} g\}$ with $\{x, w\}$ running over all edges of $\Delta_{1,1}$.

(b) From the proof above, one can see that the family $\mathcal{A}$ in Theorem 3.1 is not unique in general, and this is the case even for Frobenius graphs of the first type.

4 Gossiping

This section is devoted to the gossiping problem for which each vertex has a distinct set of m messages to be sent to all other vertices, where $m \geq 1$ is a given integer. In the following discussion we assume the *store-and-forward* model, that is, a vertex must receive a message wholly before retransmitting it to other vertices. Also, we assume that it takes one time step to transmit any message, that is, the time required to transmit a message is independent of its length. Further, we assume that during each time step a vertex can exchange messages (which may be different) with all of its neighbours simultaneously (*all-port*), and that an edge can be used to transmit messages in both directions (*full-duplex*) at the same time. Finally, to facilitate presentation of our results we make the following assumption:

(†) at each time step a vertex can send (receive) at most m messages to (from) each of its neighbours, and these messages may have different destinations (sources).

For brevity an algorithm which fulfils the gossiping task under the assumptions above is called an *m-gossiping protocol*. The assumption (†) is not as restrictive as it may look like since without it the required gossip time will be magnified by m. See Remark 4.5(b) for an explanation.

Let us first deal with the case $m \geq \delta$ in the following theorem. The other case $m < \delta$ will be treated in Corollary 4.4.

Theorem 4.1 *Let $\Gamma = \mathrm{Cay}(G, S)$ be a connected Cayley graph of degree $\delta = |S|$ and diameter d. Suppose that there exists a subgroup H of $\mathrm{Aut}(G, S)$ which is regular on S. Then for any integer $m \geq \delta$ there exists an m-gossiping protocol for Γ such that the following hold:*

(a) *messages are always transmitted along shortest paths of Γ;*

(b) *at any time t:*

(i) *each arc of* Γ *is exploited exactly once for message transmission;*

(ii) *for each* $g \in G$ *precisely* δ *arcs with different colours are used to transmit messages with source* g*, and the sets* $A_t(g)$ *of such arcs for* g *running over* G *form a partition of* $\texttt{Arc}(\Gamma)$*; and*

(iii) G *is transitive on* $\{A_t(g) : g \in G\}$*;*

(c) *the total number of time steps required to complete the gossiping is* $\sum_{i=1}^{d} n_i$*, where* n_i *is the number of* H*-orbits contained in* $\Gamma_i(1)$*.*

The promised m-gossiping protocol will be given in Algorithm 4.3. It is induced by $\mathcal{A}$ in Theorem 3.1. Special features of the spanning subgraphs in $\mathcal{A}$ when H is regular on S are summarized in the following lemma, and they will be used in the proof of Theorem 4.1 as well as the proofs of Theorems 5.1 and 6.1 in the next two sections. For a group L and a subgroup K of L, a *right transversal to* K *in* L (see e.g. [27]) is a subset U of L which contains exactly one element from each right coset of K in L.

Lemma 4.2 *Under the conditions of Theorem 4.1, let* $\mathcal{A} = \{\Delta_g : g \in G\}$ *be the family of spanning subgraphs guaranteed by Theorem 3.1, and let* R_i *be a set of representatives of the family of* H*-orbits contained in* $\Gamma_i(1)$*. Then for any* $g \in G$ *and* $1 \le i \le d-1$ *the set of arcs of* Δ_g *from* $\Gamma_i(g)$ *to* $\Gamma_{i+1}(g)$ *is given by* $\bigcup_{y \in R_{i+1}} C_g(y, v)$*, where* v *is the unique neighbour of* y *in* $\Delta_{1,1}$ *contained in* $\Gamma_i(1)$*, and*

$$C_g(y, v) = \{(v^{\phi_j \psi_\ell} g, y^{\psi_\ell} g) : 0 \le \ell \le p-1, 0 \le j \le q-1\},$$

where $p = |y^H|$*,* $q = |H_y|$*,* $H_y = \{\phi_0, \phi_1, \ldots, \phi_{q-1}\}$ $(\phi_0 = 1)$ *and* $\{\psi_0, \psi_1, \ldots, \psi_{p-1}\}$ $(\psi_0 = 1)$ *is a right transversal to* H_y *in* H*. Moreover,* $C_g(y, v) = C_1(y, v)^g$*,* $C_g(y, v)$ *is the set of arcs of* Δ_g *from* $v^H g$ *to* $y^H g$*, and the* δ *arcs in* $C_g(y, v)$ *receive distinct colours. Furthermore, if in addition* H *is semiregular on* $G \setminus \{1\}$*, then* $C_g(y, v) = \{(v^\psi g, y^\psi g) : \psi \in H\}$ *is a matching of* δ *arcs.*

Proof Since H is regular on S, $S = a^H$ is an H-orbit on G (where a is a fixed element of S), $|H| = |S| = \delta$, and the results in Theorem 3.1 apply. Let us continue the discussion in the proof of Theorem 3.1 and use the notation there. In particular, let $L_i(1) = \Gamma_i(1) \cap V(\Delta_{1,1})$, $0 \le i \le d$. For $y \in R_{i+1}$, without loss of generality we may assume $y \in L_{i+1}(1)$, so that $v \in L_i(1)$. By Theorem 3.1(d), $\Delta_1(y^H) \cap \Gamma_i(1) = v^H$ and each vertex x in y^H lies in exactly $|H_x| = |H_y| = q$ subtrees $\Delta_{1,\phi}$ $(\phi \in H)$ of Δ_1. In other words, in Δ_1 each vertex of y^H has q neighbours contained in v^H. Since $\Delta_1 = \bigcup_{\phi \in H} \Delta_{1,\phi}$, it is evident that the subtrees containing y are Δ_{1,ϕ_j} $(0 \le j \le q-1)$, and thus in Δ_1 the neighbours of y contained in v^H are v^{ϕ_j} $(0 \le j \le q-1)$. Since $\Delta_1(y^H) \cap \Gamma_i(1) = v^H$, it follows that $\Delta_1(y) \cap \Gamma_i(1) = \{v^{\phi_j} : 0 \le j \le q-1\}$. Since v is adjacent to y in Γ, we have $vy^{-1} \in S$ and hence $v = a^{\hat{\phi}} y$ for some $\hat{\phi} \in H$. Since $H \le \mathrm{Aut}(G)$ is regular on S, we have: $v^{\phi_j} = v^{\phi_{j'}} \Leftrightarrow a^{\hat{\phi}\phi_j} y^{\phi_j} = a^{\hat{\phi}\phi_{j'}} y^{\phi_{j'}} \Leftrightarrow a^{\hat{\phi}\phi_j} y = a^{\hat{\phi}\phi_{j'}} y \Leftrightarrow a^{\hat{\phi}\phi_j} = a^{\hat{\phi}\phi_{j'}} \Leftrightarrow \hat{\phi}\phi_j = \hat{\phi}\phi_{j'}$ $\Leftrightarrow \phi_j = \phi_{j'} \Leftrightarrow j = j'$. In other words, for distinct $\phi_j, \phi_{j'} \in H_y$, the neighbours $v^{\phi_j}, v^{\phi_{j'}}$ of y in Δ_1 are distinct. In general, since $\{\psi_0, \psi_1, \ldots, \psi_{p-1}\}$ $(\psi_0 = 1)$ is a right transversal to H_y in H, we have $H = \bigcup_{\ell=0}^{p-1} H_y \psi_\ell$ and $y^H = \{y^{\psi_\ell} : 0 \le \ell \le p-1\}$. Since $H_y \psi_\ell = \{\phi_j \psi_\ell : 0 \le j \le q-1\}$, $0 \le \ell \le p-1$, the subtrees containing y^{ψ_ℓ} are $\Delta_{1,\phi_j \psi_\ell}$. Hence in Δ_1 the neighbours of y^{ψ_ℓ} contained in $\Gamma_i(1)$ are $v^{\phi_j \psi_\ell}$ $(0 \le j \le q-1)$, which are pairwise distinct. Therefore, in Δ_1 the arcs from v^H to y^H are exactly those in $C_1(y,v)$, and hence the set of arcs of Δ_1 from $\Gamma_i(1)$ to $\Gamma_{i+1}(1)$ is given by $\bigcup_{y\in R_{i+1}} C_1(y,v)$. Based on this and $\Delta_g = \Delta_1^g$, we then obtain the required results for any $g \in G$ by translation, that is, $C_g(y,v) = C_1(y,v)^g$. Since $pq = |H| = \delta$, we have $|C_g(y,v)| = \delta$ and Theorem 3.1(c) ensures that the δ arcs in $C_g(y,v)$ receive distinct colours.

In the case where H is semiregular on $G \setminus \{1\}$, we have $q = 1$ for all $y \in G \setminus \{1\}$ and hence $C_g(y,v) = \{(v^{\psi}g, y^{\psi}g) : \psi \in H\}$, which is clearly a matching of δ arcs. □

As in Theorem 3.1, in Lemma 4.2 H is semiregular on $G \setminus \{1\}$ if and only if $G : H$ is a Frobenius group, and in this case Γ is a first type $G : H$-Frobenius graph. Equipped with Lemma 4.2 we now give the promised m-gossiping protocol and prove that it satisfies (a)-(c) in Theorem 4.1. A process of disseminating messages at a specific source vertex to all other vertices is called *broadcasting*.

Algorithm 4.3 We use the notation in Theorem 3.1 and Lemma 4.2. Using Δ_1 we will first give the following broadcasting algorithm (1a)-(1b) for the identity vertex 1 and then obtain the desired m-gossiping protocol by means of translations.

(1a) In the beginning the m messages at 1 are to be transmitted to all other vertices. The broadcasting goes through d phases each consisting of a number of time steps. The first phase consists of the first step only in which the m messages at 1 are transmitted to all of its neighbours a^{ϕ} ($\phi \in H$) simultaneously. In the ith phase, $2 \le i \le d$, messages are transmitted from $\Gamma_{i-1}(1)$ to $\Gamma_i(1)$ in the way to be specified in (1b).

(1b) Inductively, suppose that the ith phase has finished, that is, all vertices in $\Gamma_i(1)$ have received via $\Gamma_{i-1}(1)$ the m messages which are originated from 1. In the next phase these messages are to be transmitted from $\Gamma_i(1)$ to $\Gamma_{i+1}(1)$ such that the vertices in the same H-orbit contained in $\Gamma_{i+1}(1)$ receive messages in the same time step.

More explicitly, let $y \in R_{i+1}$ and v be as in Lemma 4.2. Then $y^H = \{y^{\psi_\ell} : 0 \le \ell \le p-1\}$, $v^H = \{v^{\phi_j \psi_\ell} : 0 \le \ell \le p-1, 0 \le j \le q-1\}$, and $C_1(y,v) = \{(v^{\phi_j\psi_\ell}, y^{\psi_\ell}) : 0 \le \ell \le p-1, 0 \le j \le q-1\}$. Split the m messages at each vertex in $\Gamma_i(1)$ into q parts, $M_0, M_1, \ldots, M_{q-1}$, such that each part contains at least $\lfloor m/q \rfloor$ and at most $\lceil m/q \rceil$ messages. Since $m \ge \delta$, we have $\lfloor m/q \rfloor \ge 1$ and thus none of these parts is empty. In the same time step, the messages in the jth part M_j are transmitted from $v^{\phi_j\psi_\ell}$ to y^{ψ_ℓ}, $0 \le \ell \le p-1$, $0 \le j \le q-1$. Thus, each vertex in y^H receives exactly one copy of each message in M_j for $0 \le j \le q-1$. By Lemma 4.2 in this time step the δ arcs in $C_1(y,v)$ are used to transmit messages from v^H to y^H, and each arc is used exactly once in this step. Moreover, by Lemma 4.2 the arcs in $C_1(y,v)$ have different colours.

For each $y \in R_{i+1}$ we apply the above so that each y^H takes one time step to receive messages from $\Gamma_i(1)$. Since R_{i+1} is a set of representatives of the family of H-orbits contained in $\Gamma_{i+1}(1)$, after all $y \in R_{i+1}$ have been treated every vertex in $\Gamma_{i+1}(1)$ receives the m messages with source 1 via $\Gamma_i(1)$.

If $i + 1 = d$, then the broadcasting is completed; otherwise set $i := i + 1$ and repeat the procedure above.

(2) Let $A_t(1)$ denote the set of arcs used in the broadcasting above at time t. Let $A_t(g) := A_t(1)^g = \{(wg, zg) : (w,z) \in A_t(1)\}$. At time t when the messages with source 1 are transmitting along the arcs in $A_t(1)$, disseminate the messages with source g along arcs in $A_t(g)$ for all $g \in G$.

Thus, in the first step ($t = 1$) the messages with source g are transmitted to all of its neighbours $a^{\phi}g$ ($\phi \in H$) simultaneously for all $g \in G$. At time $t \geq 2$, from (1a)-(1b) above we have $A_t(1) = C_1(y, v)$ for some (y, v), and hence $A_t(g) = C_g(y, v)$ by Lemma 4.2. For $0 \leq \ell \leq p - 1$ and $0 \leq j \leq q - 1$, when M_j (originating from 1) is transmitted from $v^{\phi_j \psi_\ell}$ to y^{ψ_ℓ} at time t, for all $g \in G$, M_j (originating from g) is transmitted from $v^{\phi_j \psi_\ell} g$ to $y^{\psi_\ell} g$ at the same time step. □

In (1b) above, since H is not necessarily regular on v^H, a vertex $w \in v^H$ may be written in two different ways, e.g. $w = v^{\phi_j \psi_\ell} = v^{\phi_{j'} \psi_{\ell'}}$ for $(\ell, j) \neq (\ell', j')$. If $j \neq j'$, then $v^{\phi_j} \neq v^{\phi_{j'}}$ and hence $\ell \neq \ell'$. In the case when $j = j'$ but $\ell \neq \ell'$, part M_j at w is transmitted to both y^{ψ_ℓ} and $y^{\psi_{\ell'}}$ in the same time step.

Proof of Theorem 4.1 It is easy to verify that Algorithm 4.3 gives an m-gossiping protocol for Γ. Continuing the discussion in Algorithm 4.3, for any $t \geq 2$ the set of arcs used for transmission at time t is $\bigcup_{g \in G} A_t(g) = \bigcup_{g \in G} A_t(1)^g = \bigcup_{g \in G} C_1(y, v)^g$. By Lemma 4.2 we have $|A_t(g)| = \delta$ and the arcs in $A_t(g)$ ($\subseteq \mathtt{Arc}(\Delta_g)$) have different colours. Since H is regular on S, by Lemma 2.1, Γ is $G : H$-arc transitive. For any $\phi g \in G : H$ (where $\phi \in H$ and $g \in G$), since ϕ leaves all H-orbits invariant, it leaves $A_t(1) = C_1(y, v)$ invariant. Thus, the $G : H$-arc transitivity of Γ implies that $\bigcup_{g \in G} A_t(g) = \mathtt{Arc}(\Gamma)$, that is, all arcs of Γ are used at each time t. Since Γ has exactly $\delta|G|$ arcs, it follows that $|\bigcup_{g \in G} A_t(g)| = \delta|G|$. On the other hand, since $|A_t(g)| = \delta$ for all $g \in G$, we have $\delta|G| = |\bigcup_{g \in G} A_t(g)| \leq \sum_{g \in G} |A_t(g)| = \delta|G|$. Therefore, $\{A_t(g) : g \in G\}$ must be a partition of $\mathtt{Arc}(\Gamma)$. In other words, at each time step $t \geq 2$, all arcs of Γ are used for message transmission, and moreover each arc is used exactly once. Obviously, G is transitive on $\{A_t(g) : g \in G\}$. (It may happen that at the same time step a vertex is required to process messages from different sources. This is allowed by our assumption (†).) Thus, the statements in (b) of Theorem 4.1 hold for $t \geq 2$. Clearly, these statements are true for $t = 1$ as well.

From Algorithm 4.3 it follows that all messages are transmitted along shortest paths, and the total number of time steps required is one less than the the number of H-orbits on G. In other words, the total number of steps is $\sum_{i=1}^{d} n_i$, where n_i is the number of H-orbits contained in $\Gamma_i(1)$. □

Corollary 4.4 *Let $\Gamma = \mathrm{Cay}(G, S)$ be a connected Cayley graph of degree $\delta = |S|$ and diameter d. Suppose that there exists a subgroup H of $\mathrm{Aut}(G, S)$ which is regular on S. Then for any positive integer $m < \delta$ there exists an m-gossiping protocol such that the following (a)-(c) hold:*

(a) *messages are always transmitted along shortest paths of Γ;*

(b) *at any time t:*

  (i) *each arc of Γ is used at most once for message transmission;*

  (ii) *for each $g \in G$ at most δ arcs $\hat{A}_t(g)$ with different colours are used to transmit messages with source g;*

  (iii) *G is transitive on $\{\hat{A}_t(g) : g \in G\}$;*

(c) *the total number of time steps is $\sum_{i=1}^{d} n_i$, where n_i is the number of H-orbits contained in $\Gamma_i(1)$.*

Proof Since $m < \delta$, we may add $\delta - m$ 'dummy messages' at each vertex so that Theorem 4.1 applies. The messages with source g need to be partitioned into q parts when transmitting along $C_g(y, v)$, where $q = |H_y|$ $(\leq \delta)$. Put all original messages into the first $\lceil m/q \rceil$ parts, so that the dummy messages are in the remaining parts and possibly in the $\lceil m/q \rceil$th part. In Algorithm 4.3 the arcs $(v^{\phi_j \psi_\ell} g, y^{\psi_\ell} g)$ $(0 \leq i \leq p-1,\ 0 \leq j \leq \lceil m/q \rceil - 1)$ are the only ones in $C_g(y, v)$ which carry the original messages. Thus, at each time step t the set $\hat{A}_t(g)$ of arcs carrying the original messages is a subset of $A_t(g)$. The results follow from Theorem 4.1 immediately by ignoring those parts which contain dummy messages only. □

Remark 4.5 (a) From the well-known Cauchy-Frobenius Lemma (e.g. [9, Theorem 1.7A]), in Theorem 4.1 and Corollary 4.4 the total number of steps required can be also expressed as $(\sum_{\phi \in H} |\mathrm{fix}(\phi)|)/|H| - 1$, where $\mathrm{fix}(\phi) = \{g \in G : g^\phi = g\}$.

(b) Using Theorem 4.1(c) one can easily obtain the total number of steps required when the assumption (†) is removed. For example, if at each time step a vertex can send (receive) at most one message to (from) its neighbours, then we need at most m steps to complete transmission from v^H to y^H and hence the total number of steps is at most $m \sum_{i=1}^{d} n_i$.

(c) Let us emphasize that, since all results in this section are valid for any Cayley graph in class **R**, they are all valid for any Cayley graph admitting a complete rotation (Figure 2).

(d) In this section we discussed only the store-and-forward, all-port and full-duplex model. Based on Theorem 3.1 one may modify the method above to obtain gossiping protocols under other communication models such as the (i, j) mode [21, Section 5.4] and the c-port model [15].

5 Minimum gossip time

In this section we consider the gossiping problem with $m = 1$, that is, each vertex has exactly one message to transmit to other vertices. This is the case that receives most attention in the literature. As in the previous section we assume the store-and-forward, all-port and full-duplex model, and each vertex can send (receive) at most one message to (from) each of its neighbours at each time step. In addition we assume that no two messages can transmit over the same arc at the same time. An algorithm which fulfils the gossiping task under these assumptions will be called a *gossiping protocol*. Denote by $t(\Gamma)$ the minimum number of time steps required by such a protocol. (Thus, $t(\Gamma)$ is the *minimum gossip time* $g_{F_*}(1, \Gamma)$ discussed in [4].) A gossiping protocol is called *optimal* if uses $t(\Gamma)$ time steps.

The main results in this section generalise two results in [4] to a wider class of Cayley graphs. For any regular graph Γ of degree δ, since any vertex v can receive at most δ messages at each time step and in total there are $|V(\Gamma)| - 1$ messages to be transmitted to v, it follows ([4, Proposition 7] and [13, Lemma 16]) that

$$t(\Gamma) \geq \left\lceil \frac{|V(\Gamma)| - 1}{\delta} \right\rceil. \tag{6}$$

The next theorem shows that this trivial lower bound is attained by all Frobenius graphs of the first type, or equivalently Cayley graphs $\mathrm{Cay}(G, S)$ such that H is regular on S and semiregular on $G \setminus \{1\}$ for some $H \leq \mathrm{Aut}(G, S)$. Note that in Theorem 4.1 we assumed $m \geq \delta$ in order to facilitate presentation. However, in Algorithm 4.3 what we really used was that $m \geq |H_y|$ for each $y \in G \setminus \{1\}$ so that all $M_j \neq \emptyset$. Under the assumption that H is semiregular on $G \setminus \{1\}$ we have $|H_y| = 1$ and hence an algorithm similar to Algorithm 4.3 works well for $m = 1$.

Theorem 5.1 *Let $L = G : H$ be a Frobenius group with Frobenius kernel G, where H is a Frobenius complement of G in L. Let $\Gamma = \mathrm{Cay}(G, S)$ be a first type L-Frobenius graph of degree $\delta = |S|$, where $S = a^H$ for some $a \in G$ with $\langle a^H \rangle = G$ and $|H|$ is even or $|a| = 2$. Then the minimum gossip time of Γ is given by*

$$t(\Gamma) = \frac{|G| - 1}{\delta}. \tag{7}$$

Moreover, there exists an optimal gossiping protocol for Γ such that the following (a)-(b) hold:

(a) *messages are always transmitted along shortest paths of Γ;*

(b) *at any time t:*

  (i) *each arc of Γ is used exactly once for message transmission;*

  (ii) *for each $g \in G$ exactly δ arcs with different colours are used to transmit messages with source g, the set $A_t(g)$ of such arcs form a matching of Γ, and moreover $\{A_t(g) : g \in G\}$ is a partition of $\mathtt{Arc}(\Gamma)$;*

  (iii) *G is transitive on $\{A_t(g) : g \in G\}$.*

Proof Since H is regular on S, we have $\delta = |S| = |H|$ and the results in Theorem 3.1 hold for (Γ, G). In particular, by Theorem 3.1 the subgraphs Δ_g $(g \in G)$ are shortest path spanning trees of Γ. Applying Lemma 4.2 and using the notation there, by the semiregularity of H on $G \setminus \{1\}$ we have $p = |x^H| = |H| = |S| = \delta$ and $q = |H_x| = 1$ for all $x \in G \setminus \{1\}$, and each $C_g(y, v) = \{(v^\psi g, y^\psi g) : \psi \in H\}$ is a matching of δ arcs. Algorithm 5.2 below is a modification of Algorithm 4.3, and it gives the required gossiping protocol. The difference is that in the current situation there is only one message originating from each vertex and each $C_g(y, v)$ is a matching.

Algorithm 5.2 As in Algorithm 4.3, at time $t = 1$ the messages with source g are transmitted to all of its neighbours $a^\phi g$ $(\phi \in H)$ simultaneously for all $g \in G$. In the $(i + 1)$th phase the message with source g is transmitted from $\Gamma_i(g)$ to $\Gamma_{i+1}(g)$ for $g \in G$. For $g = 1$ this is achieved simply by sending the message with source 1 along the arcs of $C_1(y, v)$ (that is, from v^ψ to y^ψ, $\psi \in H$) at the same time step, and we do this for all $y \in R_{i+1}$ such that each y^H takes one time step, where as in Lemma 4.2 R_{i+1} is a set of representatives of the family of H-orbits contained in $\Gamma_{i+1}(1)$. Suppose $C_1(y, v)$ is used for transmission at time $t \geq 2$, so that $A_t(1) = C_1(y, v)$. Then for each $g \in G$ let $A_t(g) := A_t(1)^g = C_1(y, v)^g = C_g(y, v)$, and at the same time t transmit the message with source g along the arcs in $A_t(g)$ (that is, from $v^\psi g$ to $y^\psi g$, $\psi \in H$). □

By Lemma 4.2 $A_t(g)$ is a matching of Δ_g with its δ arcs having different colours. Note that the message with source g is transmitted along shortest paths to other vertices since Δ_g is a shortest path spanning tree. Similar to the proof of Theorem 4.1, one can verify that $\{A_t(g) : g \in G\}$ is a partition of $\mathtt{Arc}(\Gamma)$, G is transitive on $\{A_t(g) : g \in G\}$, and each arc of Γ is used exactly once at each time t. Thus, Algorithm 5.2 is indeed a gossiping protocol satisfying (a) and (b) in Theorem 5.1. Since all H-orbits in $G\setminus\{1\}$ have length δ as shown above and each H-orbit needs one time step, this gossiping protocol requires $(|G|-1)/\delta$ steps in total. Hence $t(\Gamma) \le (|G|-1)/\delta$. This together with (6) yields $t(\Gamma) = (|G|-1)/\delta$ and implies that the protocol is optimal. □

In the following we discuss the more general case where H is not necessarily semiregular on $G \setminus \{1\}$. We still assume that H is regular on S, so that $|H| = |S| = \delta$. Thus, by the orbit-stabiliser lemma, an H-orbit x^H on $G\setminus\{1\}$ has length δ if and only if $H_x = 1$, and in this case $H_u = 1$ for all $u \in x^H$. Let

$$X := \{x \in G : H_x = 1\} \cup \{1\}.$$

Then $X \setminus \{1\}$ is the union of all H-orbits on $G \setminus \{1\}$ of length δ. Thus, δ is a divisor of $|X| - 1$. Since H is semiregular on $G \setminus \{1\}$ if and only if $X = G$, Theorem 5.3 below can be viewed as a generalisation of Theorem 5.1. It also generalises [4, Lemma 17], which itself was very useful [4] in determining the exact values of the minimum gossip time for hypercubes, multidimensional tori and star graphs. An *independent set* of a graph is a set of pairwise nonadjacent vertices of the graph, and a *vertex-cut* is a subset of the vertex set whose removal increases the number of connected components.

Theorem 5.3 *Let $\Gamma = \mathrm{Cay}(G, S)$ be a connected Cayley graph with degree $\delta = |S|$. Suppose that there exists $H \le \mathrm{Aut}(G, S)$ such that H is regular on S and that $G \setminus X$ is an independent set and not a vertex-cut of Γ, where $X = \{x \in G : H_x = 1\} \cup \{1\}$ as above. Then the minimum gossip time of Γ is given by*

$$t(\Gamma) = \left\lceil \frac{|G|-1}{\delta} \right\rceil. \tag{8}$$

Moreover, we can give an optimal gossiping protocol for Γ under which messages are transmitted along shortest paths.

Proof Since H is regular on S, we have $|H| = |S| = \delta$. Let $\Gamma[X]$ denote the subgraph of Γ induced on X. Since $G \setminus X$ is not a vertex-cut of Γ, $\Gamma[X]$ is connected. Since $G \setminus X$ is an independent set, any edge with one end-vertex in $G \setminus X$ must have the other end-vertex in X and hence is in the edge-cut $\delta(X, G \setminus X)$ (that is, the set of edges of Γ between X and $G \setminus X$). Note that $X \setminus \{1\}$ is the union of H-orbits y^H on G with $H_y = 1$, and $G \setminus X$ is the union of H-orbits z^H on G with $H_z \ne 1$. Note also that each $\Gamma_i(1)$, $0 \le i \le d$, is a union of H-orbits on G. (See Claim 1 in the proof of Theorem 3.1.) Thus, for each $z^H \subseteq G \setminus X$ there exists a unique i such that $z^H \subseteq \Gamma_{i+1}(1)$ and $\Gamma(z^H) \subseteq X \cap \Gamma_i(1)$.

For each $y^H \subseteq X \setminus \{1\}$, say, $y^H \subseteq \Gamma_{i+1}(1)$, by the connectedness of $\Gamma[X]$ there exists v^H such that $v^H \subseteq X \cap \Gamma_i(1) \cap \Gamma(y^H)$. Without loss of generality we may assume that v is the unique neighbour of y in $\Delta_{1,1}$. Since $|H_y| = 1$, from Lemma 4.2 the set of arcs of Γ from v^H to y^H is $C_1(y, v) = \{(v^\psi, y^\psi) : \psi \in H\}$. Thus, we can apply Algorithm 5.2 but restrict to X so that at each time step transmission takes place over one $C_1(y, v)$. Since each y^H contained in $X \setminus \{1\}$ has length δ, the message with source 1 can reach all vertices in X in $t_0 := (|X| - 1)/\delta$ time steps, and moreover it transmits along shortest paths. Now let us partition $G \setminus X$ into $t_1 := \lceil (|G| - |X|)/\delta \rceil$ parts, $V_1, \ldots, V_{t_1}$, such that $|V_1| = \cdots = |V_{t_1 - 1}| = \delta$ and $|V_{t_1}| \le \delta$. For

$1 \le i \le t_1$, choose an injection $\theta_i : V_i \to S$, which can be taken as an assignment of δ colours (elements of S) to the vertices in V_i such that different vertices receive distinct colours. (For $1 \le i \le t_1 - 1$, θ_i is in fact a bijection since $|V_i| = \delta$. Similarly, θ_{t_1} is a bijection when $|V_{t_1}| = \delta$.) For each i, since all δ colours appear on the δ arcs incident with each vertex in V_i, we can choose a set C_i of $|V_i|$ arcs of Γ such that each $z \in V_i$ is incident with exactly one arc $(w, z) \in C_i$ and that $zw^{-1} = \theta_i(z)$, where w is necessarily in X. From the choice of θ_i it follows that such arcs $(w, z) \in C_i$ receive different colours. However, for distinct $z, z' \in V_i$, it is allowed to have $w \neq w'$ for corresponding arcs $(w, z), (w', z') \in C_i$. At time $t_0 + i$ we simply transmit the message with source 1 from X to V_i along the arcs in C_i, $1 \le i \le t_1$. Thus, we can broadcast the message with source 1 to all other vertices in $t_0 + t_1 = \lceil (|G| - 1)/\delta \rceil$ steps. From the discussion in the first paragraph one can see that this broadcasting uses shortest paths for transmission.

For $g \in G$, $Xg = \{xg : x \in X\}$ induces a connected subgraph of Γ isomorphic to $\Gamma[X]$, and $G \setminus Xg$ is an independent set and not a vertex-cut of Γ. At the time when the message with source 1 is transmitted from a vertex u to a vertex x, the message with source g is transmitted from ug to xg for all $g \in G$. To show that this is indeed a gossiping protocol, it suffices to prove that at the same step two messages do not compete for the same arc. Let us consider $t \le t_0$ first. Suppose otherwise and let, say, the messages with sources 1 and $g \neq 1$ use the same arc $(v^{\psi}, y^{\psi}) = (v^{\psi'} g, y^{\psi'} g)$ at the same time, where $\psi, \psi' \in H$. Then $v^{\psi} = v^{\psi'} g$, $y^{\psi} = y^{\psi'} g$, and hence $(vy^{-1})^{\psi} = (vy^{-1})^{\psi'}$. Since $vy^{-1} \in S$ and H is regular on S, we have $\psi = \psi'$ and so $g = 1$, a contradiction. Thus, each arc is used to transmit at most one message at any time $t \le t_0$. It remains to deal with times after t_0. Suppose, say, the messages with sources 1 and g use the same arc $(w, z) = (ug, xg)$ at time $t_0 + i$, where $x, z \in V_i$ and $(u, x), (w, z) \in C_i$. Then $ux^{-1} = zw^{-1}$, that is, $\theta_i(x) = \theta_i(z)$, contradicting the choice of C_i. Thus, no two messages with different sources use the same arc at time $t_0 + i$, $1 \le i \le t_1$. Therefore, the scheme above is a gossiping protocol indeed. Moreover, messages are transmitted along shortest paths since this is the case for the broadcasting described in the previous paragraph. Clearly, the gossiping protocol requires $t_0 + t_1 = \lceil (|G| - 1)/\delta \rceil$ steps. Hence $t(\Gamma) \le \lceil (|G| - 1)/\delta \rceil$, which together with (6) yields (8) and ensures that the protocol is optimal. □

Remark 5.4 Let $\Gamma = \mathrm{Cay}(G, S)$ admit a complete rotation $\phi \in \mathrm{Aut}(G, S)$. Then $a^{\langle \phi \rangle} = S$ for some $a \in S$ and $\langle \phi \rangle \le \mathrm{Aut}(G, S)$ is regular on S. In this special case, Theorems 5.1 and 5.3 give [4, Corollary 15] and [4, Lemma 17], respectively.

6 Forwarding indices

An *all-to-all routing* (or *routing* for short) of a graph $\Gamma = (V(\Gamma), E(\Gamma))$ is a set $\mathcal{P}$ of oriented paths of Γ such that for each ordered pair $x, y \in V(\Gamma)$, $x \neq y$, there is exactly one path in $\mathcal{P}$ from x to y. The load of an edge under $\mathcal{P}$ is the number of paths in $\mathcal{P}$ going through the edge in either direction, and the load of an arc is defined similarly with direction taking into account. A routing $\mathcal{P}$ is *edge-uniform* (*arc-uniform*, respectively) if all edges (arcs, respectively) have the same load, and is a *shortest path routing* if each path in $\mathcal{P}$ is a shortest path between the end-vertices. Let $\pi(\Gamma, \mathcal{P})$ ($\overrightarrow{\pi}(\Gamma, \mathcal{P})$, respectively) be the maximum load on an edge (arc, respectively) of Γ under $\mathcal{P}$. Call

$$\pi(\Gamma) := \min_{\mathcal{P}} \pi(\Gamma, \mathcal{P}), \quad \overrightarrow{\pi}(\Gamma) := \min_{\mathcal{P}} \overrightarrow{\pi}(\Gamma, \mathcal{P})$$

the *edge-* and *arc-forwarding indices* of Γ [20] respectively, where the minimum is taken over all possible routings of Γ. If the minimum is restricted to shortest path routings, we obtain $\pi_m(\Gamma)$ and $\overrightarrow{\pi}_m(\Gamma)$, the *minimal edge-* and *arc-forwarding indices* [18] of Γ. It is clear that $\pi(\Gamma) \le 2\overrightarrow{\pi}(\Gamma)$ and $\pi_m(\Gamma) \le 2\overrightarrow{\pi}_m(\Gamma)$, and the equalities do not hold in general. A routing achieving $\pi(\Gamma)$ is said to be *optimal* for π, and similar terminology will be used for $\overrightarrow{\pi}$, π_m and $\overrightarrow{\pi}_m$. For a routing $\mathcal{P}$ and a subgroup G of $\mathrm{Aut}(\Gamma)$, if G leaves $\mathcal{P}$ *invariant* (that is, $P \in \mathcal{P}$ implies $P^g \in \mathcal{P}$ for $g \in G$) and is transitive on $E(\Gamma)$ ($\mathtt{Arc}(\Gamma)$, respectively), then $\mathcal{P}$ is said [24] to be a *G-edge transitive routing* (*G-arc transitive routing*, respectively).

In general it is difficult to determine the indices above (see e.g. [18, Section 5]). For any Frobenius graph Γ (regardless of its type), it was proved [30, Theorem 2.2] that $\pi(\Gamma) = (\sum_{(u,v)\in G\times G} d(u,v)/|E(\Gamma)|$, and this was obtained under the name of orbital regular graphs. A second formula for $\pi(\Gamma)$ was given in [11, Theorem 1.6] for Frobenius graphs, namely, $\pi(\Gamma) = 2\sum_{i=1}^{d} in_i$ or $\sum_{i=1}^{d} in_i$, depending on whether Γ is of the first or second type, where n_i is the number of H-orbits contained in $\Gamma_i(1)$. However, as far as we know no optimal routing for π is known in the literature. Using Theorem 3.1, for Frobenius graphs Γ of the first type we now give a shortest path routing which exhibits interesting features and is optimal for π, $\overrightarrow{\pi}$, $\overrightarrow{\pi}_m$ and π_m simultaneously.

Theorem 6.1 *Let $L = G : H$ be a Frobenius group with Frobenius kernel G, where H is a Frobenius complement of G in L. Let $\Gamma = \mathrm{Cay}(G, S)$ be a first type L-Frobenius graph, where $S = a^H$ for some $a \in G$ with $\langle a^H \rangle = G$ and $|H|$ is even or $|a| = 2$. Then*

$$\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = \frac{\sum_{(u,v)\in G\times G} d(u,v)}{|E(\Gamma)|}. \tag{9}$$

Denote by $\mathcal{P}$ the routing obtained from $\mathcal{A} = \{\Delta_g : g \in G\}$ (guaranteed by Theorem 3.1) such that for any $g, x \in G$ the route from g to x is the unique path from g to x in the shortest path spanning tree Δ_g of Γ. Then $\mathcal{P}$ is

(a) *a shortest path routing;*

(b) *L-arc transitive;*

(c) *both edge-uniform and arc-uniform; and*

(d) *optimal for π, $\overrightarrow{\pi}$, $\overrightarrow{\pi}_m$ and π_m simultaneously.*

As mentioned above, the value of $\pi(\Gamma)$ is known in the literature. However, the value of $\overrightarrow{\pi}(\Gamma)$ above is new. In [20, Theorem 3.2] it was shown that

$$\pi_m(\Gamma) \ge \pi(\Gamma) \ge \frac{\sum_{(u,v)\in V\times V} d(u,v)}{|E(\Gamma)|} \tag{10}$$

and the equalities hold if and only if Γ admits an edge-uniform shortest path routing. Similarly, one can verify that

$$\overrightarrow{\pi}_m(\Gamma) \ge \overrightarrow{\pi}(\Gamma) \ge \frac{\sum_{(u,v)\in V\times V} d(u,v)}{2|E(\Gamma)|} \tag{11}$$

and the equalities hold if and only if Γ admits an arc-uniform shortest path routing.

Lemma 6.2 *Let $\mathcal{P}$ be a routing for a graph Γ. If $\mathcal{P}$ is G-arc transitive for some $G \le \mathrm{Aut}(\Gamma)$, then it is also G-edge transitive, and is both arc- and edge-uniform. If in addition $\mathcal{P}$ is a shortest path routing, then $\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = (\sum_{(u,v)\in G\times G} d(u,v))/|E(\Gamma)|$ and $\mathcal{P}$ is optimal with respect to the four indices simultaneously.*

Proof Since $\mathcal{P}$ is G-arc transitive, G leaves $\mathcal{P}$ invariant and is transitive on $\mathtt{Arc}(\Gamma)$. Hence G is also transitive on $E(\Gamma)$. Since Γ is G-arc transitive, for any $(u,v),(u',v') \in \mathtt{Arc}(\Gamma)$ there exists $g \in G$ such that $(u,v)^g = (u',v')$. If $P \in \mathcal{P}$, then $P^g \in \mathcal{P}$ as $\mathcal{P}$ is G-invariant; and if P goes through (u,v) in its direction, then P^g goes through (u',v') in its direction. Based on this one can show that there is a one-to-one correspondence between the paths of $\mathcal{P}$ going through (u,v) and that going through (u',v'). It follows that (u,v) and (u',v') have the same load under $\mathcal{P}$, and hence $\mathcal{P}$ is arc-uniform. This implies that $\mathcal{P}$ is also edge-uniform since the load on $\{u,v\}$ is the sum of the loads on (u,v) and (v,u). Therefore, if in addition $\mathcal{P}$ is a shortest path routing, then by (10)-(11) we have $\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = (\sum_{(u,v)\in G\times G} d(u,v))/|E(\Gamma)|$ and thus $\mathcal{P}$ is optimal with respect to all these indices. □

Proof of Theorem 6.1 Since $L = G : H$ is a Frobenius group and $\Gamma = \mathrm{Cay}(G,S)$ is a first type L-Frobenius graph, the results in Theorem 3.1 hold for (Γ, G) and in particular $\mathcal{A} = \{\Delta_g : g \in G\}$ is a family of shortest path spanning trees of Γ. Let $\mathcal{P}$ be the routing under which for any $g, x \in G$ the route from g to x is the unique path of Δ_g from g to x. Of course $\mathcal{P}$ is a shortest path routing. For any $g \in G$ and $\psi f \in L$, where $\psi \in H$ and $f \in G$, since G is normal in L we have $g\psi = \psi g'$ for some $g' \in G$. Thus, since $\Delta_g = \bigcup_{\phi\in H}(\Delta_{1,1})^{\phi g}$ by Theorem 3.1(b), we have $\Delta_g^{\psi f} = \bigcup_{\phi\in H}(\Delta_{1,1})^{\phi g\psi f} = \bigcup_{\phi\in H}(\Delta_{1,1})^{\phi\psi g' f} = \Delta_{g'f}$. Therefore, $\mathcal{A}$ is L-invariant and hence $\mathcal{P}$ is L-invariant as well. Since Γ is L-transitive by Lemma 2.1, it follows that $\mathcal{P}$ is an L-arc transitive routing. Thus, by Lemma 6.2, $\mathcal{P}$ is L-edge transitive and both edge- and arc-unform. Again by Lemma 6.2, (9) holds and $\mathcal{P}$ is optimal for π, $\overrightarrow{\pi}$, $\overrightarrow{\pi}_m$ and π_m simultaneously. □

Remark 6.3 For a first type Frobenius graph $\Gamma = \mathrm{Cay}(G,S)$ as in Theorem 6.1, an algorithm similar to Algorithm 5.2 can be used to construct $\mathcal{A} = \{\Delta_g : g \in G\}$: in a typical step we simply construct $C_g(y,v)$ for all $g \in G$. Obviously, this algorithm terminates in $(|G|-1)/\delta$ steps, and it produces the optimal routing $\mathcal{P}$ in Theorem 6.1.

The arc-forwarding index is useful [8] in bounding the second largest eigenvalue β_1 of random walks on a connected graph. It is known [8, Corollary 1] that $\beta_1(\Sigma) \le 1 - (2|E(\Sigma)|/\delta^2 d\overrightarrow{\pi}_m(\Sigma))$ for any connected graph Σ with diameter d and maximum degree δ. When Σ is regular, this can be translated into an upper bound on the second largest eigenvalue λ_1. From this bound and the value of $\overrightarrow{\pi}_m$ implied in (9) and [11, Theorem 1.6], we obtain (12) below for any Frobenius graph of the first type. This in turn implies (13) by using the well-known Cheeger's inequality [2] $h(\Sigma) \ge (\delta - \lambda_1(\Sigma))/2$ on the *edge expansion ratio* of Σ defined by $h(\Sigma) = \min_{S\subseteq V(\Sigma), |S|\le|V(\Sigma)|/2} |\delta(S)|/|S|$, where $\delta(S)$ is the set of edges of Σ from S to $V(\Sigma)\setminus S$.

Corollary 6.4 *Let $L = G : H$ and $\Gamma = \mathrm{Cay}(G,S)$ be as in Theorem 6.1. Let d be the diameter of Γ and n_i the number of H-orbits on G at distance i from 1 in Γ, $1 \le i \le d$. Then*

$$\lambda_1(\Gamma) \le |H| - \frac{|G|}{d\sum_{i=1}^{d} i n_i} \tag{12}$$

$$h(\Gamma) \geq \frac{|G|}{2d\sum_{i=1}^{d} in_i}. \quad (13)$$

7 An example

Example 7.1 Let q be a prime power and $\mathbf{F}_q$ the finite field of order q. Then the Hamming graph $H(d,q)$ is isomorphic to $\mathrm{Cay}(\mathbf{F}_q^d, S)$, where S is the set of vectors of $\mathbf{F}_q^d$ with exactly one nonzero coordinate. As noticed in [24], $\mathrm{Aut}(\Gamma)$ contains $\mathbf{F}_q^d : G_0$ as a subgroup, where $G_0 = \mathrm{GL}(1,q) \,\mathrm{wr}\, S_d$ which fixes the identity $\mathbf{0}$ of $\mathbf{F}_q^d$. Following [24], let $x := (\alpha, 1, \ldots, 1) \cdot \tau^{-1} \in G_0$ and $H := \langle x \rangle$, where α is a prime element of $\mathbf{F}_q$ and $\tau = (1, 2, \ldots, d) \in S_d$. Then $H \cong \mathbf{Z}_{d(q-1)}$ and H is regular on S by [24, Lemma 4.2]. In [24, Theorem 1.2] it is proved that H is semiregular on $\mathbf{F}_q^d \setminus \{\mathbf{0}\}$ if and only if each prime divisor of d divides $q-1$, and in this case $H(d,q)$ is an L-Frobenius graph [24, Theorem 1.3], where $L := \mathbf{F}_q^d : H$. For any $(y_1, y_2, \ldots, y_d) \in \mathbf{F}_q^d$, we have $(y_1, y_2, \ldots, y_d)^x = (y_2, \ldots, y_d, \alpha y_1)$ as used in [24]. Hence for any $j = kd + r$ with $0 \leq k \leq q-2$ and $0 \leq r \leq d-1$ we have

$$(y_1, y_2, \ldots, y_d)^{x^j} = (\alpha^k y_{r+1}, \ldots, \alpha^k y_d, \alpha^r y_1, \ldots, \alpha^r y_r). \quad (14)$$

In particular, for $(0, \ldots, 0, s_i, 0, \ldots, 0) \in S$, where $s_i \in \mathbf{F}_q^*$,

$$(0, \ldots, 0, s_i, 0, \ldots, 0)^{x^j} = (0, \ldots, 0, \overbrace{\alpha^k s_i}^{c(i,r)}, 0, \ldots, 0), \quad (15)$$

where $c(i,r)$ is defined to be $i - r$ if $r < i$, d if $r = i$, and $(d + i - r)$ if $r > i$. Let $H(d,q)_j(\mathbf{0})$ be the set of vertices at distance j from $\mathbf{0}$, $0 \leq j \leq d$. Then $|H(d,q)_j(\mathbf{0})| = \binom{d}{j}(q-1)^j$ for each j. Since $|H| = |S| = d(q-1)$, it follows that $H(q,d)_j(\mathbf{0})$ is a union of $\binom{d}{j}(q-1)^{j-1}/d$ H-orbits on $\mathbf{F}_q^d$, $1 \leq j \leq d$. Moreover, the total distance in $H(d,q)$ between ordered pairs of distinct vertices is equal to $d(q-1)q^{2d-1}$. Since $H(d,q)$ is an L-Frobenius graph of the first type, by specifying Algorithm 5.2 and its companion outlined in Remark 6.3, we can give an algorithm for constructing the family $\mathcal{A}$ of shortest path spanning trees $\Delta_{\mathbf{g}}$ of $H(d,q)$, $\mathbf{g} \in \mathbf{F}_q^d$. The rules (14)-(15) will be useful in constructing the matching $C_{\mathbf{0}}(\mathbf{y}, \mathbf{v})$ in Lemma 4.2, where $\mathbf{y} \in H(d,q)_{j+1}(\mathbf{0}), \mathbf{v} \in H(q,d)_j(\mathbf{0})$ are adjacent in $H(d,q)$. As shown in Sections 5-6, $\mathcal{A}$ induces an optimal gossiping protocol as well as an optimal routing for $H(d,q)$. Here we have to omit computational details due to limited space. □

In summary, [24, Theorem 1.3] and the results in the previous sections imply the following corollary. Note that, since each prime divisor of d divides $q-1$, d is a divisor of $(q^d-1)/(q-1)$.

Corollary 7.2 *Let q be a prime power and $d \geq 2$ an integer. Suppose that each prime divisor of d divides $q-1$. Then all results in Theorems 3.1, 4.1, 5.1, 6.1 and Corollary 4.4 hold for $H(d,q)$. In particular, we can construct a family $\mathcal{A} = \{\Delta_{\mathbf{g}} : \mathbf{g} \in \mathbf{F}_q^d\}$ of shortest path spanning trees of $H(d,q)$ (Theorem 3.1) which gives rise to an optimal gossiping protocol and a shortest path routing (Theorem 6.1) optimal for π, $\overrightarrow{\pi}$, $\overrightarrow{\pi}_m$ and π_m simultaneously. Moreover,*

$$\pi(H(d,q)) = 2\overrightarrow{\pi}(H(d,q)) = 2\overrightarrow{\pi}_m(H(d,q)) = \pi_m(H(d,q)) = 2q^{d-1}$$

and the minimum gossip time of $H(d,q)$ is given by

$$t(H(d,q)) = \frac{q^d - 1}{(q-1)d}.$$

Remark 7.3 (a) The value of $\pi(H(d,q))$ is not new since it follows from [30, Theorem 2.2] and the main results of [24] immediately.

(b) As a special case we notice that for $d = 2$ and any odd prime power q, all the good things in Corollary 7.2 occur for $H(2,q)$ since 2 is a divisor of $q-1$. Clearly, $\pi(H(2,q)) = 2q$ and $t(H(2,q)) = (q+1)/2$. The order q^2 of $H(2,q)$ is larger than half of the well-known Moore bound (see e.g. [25]) $M_{2(q-1),2} = 2(q-1)^2 + 1$ for degree $2(q-1)$ and diameter 2, and this is probably good enough for practical purpose. Considering this and the very small diameter of $H(2,q)$, as well as all the attractive features above, it seems that $H(2,q)$ when q is an odd prime power is an attractive candidate for interconnection networks. Besides, it has the advantage of being arc-transitive.

8 Concluding remarks

In this paper we studied the class of Cayley graphs $\mathrm{Cay}(G,S)$ such that the setwise stabiliser of S in $\mathrm{Aut}(G)$ contains a subgroup which is regular on S. With motivations from communication we developed a general framework for constructing a family of connected spanning subgraphs of any Cayley graph in the class, and demonstrated that such spanning subgraphs play a key role in designing efficient gossiping protocols and optimal routings. In particular, for a large subclass of Cayley graphs associated with Frobenius groups, these spanning subgraphs are shortest path spanning trees, and they give rise to optimal gossiping protocols under the store-and-forward, all-port and full-duplex model as well as optimal shortest path routings with respect to the edge- and arc-forwarding indices. The results obtained in the paper are general in nature and thus can be applied to a number of networks, including those which admit a complete rotation. In [31] Thomson and the author have applied the method developed in the present paper to degree-six circulant graphs (that is, triple-loop networks [17]) with a given diameter and maximum possible number of vertices. We prove that such graphs are Frobenius graphs of the first type, and we give the exact values of their minimum gossip time and forwarding indices together with optimal gossiping protocols and routing schemes. In [32] we classify Frobenius circulant graphs of degree four and give their optimal gossiping and routing schemes explicitly.

In a more general setting it seems interesting to investigate existence of some connected spanning subgraphs of a Cayley graph which have 'nice' structure needed to guarantee efficient communication. Of course for different communication problems the requirements on the structure of such spanning subgraphs may be different. Problems of this type are interesting from a theoretic point of view as well; for example, the well-known Hamiltonicity problem for Cayley graphs has been well-studied over many years.

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] N. Alon and V. .D. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators, *J. Combin. Theory Ser. B* **38** (1985), no. 1, 73-88.

[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, T. Kodate and S. Perennes, Gossiping in Cayey 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.

[5] N. L. Biggs, *Algebraic Graph Theory (Second edition)*, Cambridge Mathematical Library (Cambridge University Press, Cambridge, 1993).

[6] F. Chung, E. Coffman, M. Reiman and B. Simon, On the capacity and vertex-forwarding index of communication networks, *IEEE Trans. Inform. Theory* **33** (1987), 224-232.

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

[8] P. Diaconis and D. Stroock, Geometric bounds for eigenvalues of random chains, *Ann. Applied Prob.* **1** (1991), 36-61.

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

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

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

[12] P. Fragopoulou, Communication and fault tolerance algorithms on a class of interconnection networks, Ph.D. Thesis, Queen's University, Kingston, Canada, 1995.

[13] 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.

[14] P. Fragopoulou, S. G. Akl and H. Meijer, Optimal communication primitives on the generalized hypercube networks, *J. Parallel and Distributed Computing* **32**(2) (1996), 173-187.

[15] M. Flammini and S. Pérennès, Lower bounds on the braodcasting and gossiping time of restricted protocols, *SIAM J. Discrete Math.* **17** (2004), 521-540.

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

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

[18] 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.

[19] M. C. Heydemann, N. Marlin and S. Pérennès, Complete rotations in Cayley graphs, *Europ. J. Combinatorics* **22** (2001), 179-196.

[20] M. C. Heydemann, J. C. Meyer and D. Sotteau, On forwarding indices of networks, *Discrete Applied Math.* **23** (1989), 103-123.

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

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

[23] 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.

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

[25] M. Miller and J. Širáň, Moore graphs and beyond: a survey, *The Elect. J. Combin.* (2005), #DS14.

[26] J-H. Park and K-Y. Chwa, Recursive circulants and their embeddings among hypercubes, *Theoret. Comput. Sci.* **244** (2000), 35-62.

[27] J. S. Rose, *A Course on Group Thoery*, Cambridge University Press, Cambridge, 1978.

[28] S. T. Schibell and R. M. Stafford, Processor interconnection networks from Cayley graphs, *Discrete Appl. Math.* **40** (1992), 333-357.

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

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

[31] A. Thomson and S. Zhou, Gossiping and routing in undirected triple-loop networks, submitted.

[32] A. Thomson and S. Zhou, Frobenius circulant graphs of valency four, submitted.