Gossiping and routing in second-kind Frobenius graphs

Sanming Zhou

Department of Mathematics and Statistics
The University of Melbourne
Australia
sanming@unimelb.edu.au

Joint work with Xin Gui Fang

SODO 2012, Queenstown, NZ
February 13, 2012

Motivation

Question

Which network topologies can assure high performance?

Motivation

Question

Which network topologies can assure high performance?

- Answer depends on how we measure performance

Motivation

Question

Which network topologies can assure high performance?

- Answer depends on how we measure performance
- We consider two measures:
  - minimum gossiping time
  - minimum edge-congestion for all-to-all routing

Motivation

Question

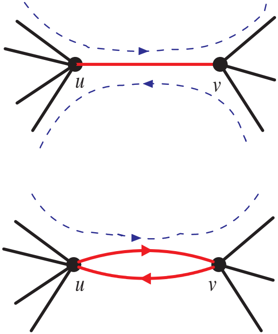
Which network topologies can assure high performance?

- Answer depends on how we measure performance
- We consider two measures:
  - minimum gossiping time
  - minimum edge-congestion for all-to-all routing
- What are the 'most efficient' graphs (of small valency) with respect to these measures?

Routing

Design a transmission route (oriented path) for each ordered pair of vertices in a given network $\Gamma = (V, E)$.

- A set $\mathcal{R}$ of such oriented paths is called an all-to-all routing
- Load of an edge = number of paths traversing the edge in either direction
- Load of an arc = number of paths traversing the arc in its direction, an arc being an ordered pair of adjacent vertices



Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load on an edge
- Edge-forwarding index $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$
- Minimal e.f. index $\pi_m(\Gamma)$: same as $\pi(\Gamma)$ but use shortest paths only
- $\overrightarrow{L}(\Gamma, \mathcal{R})$ = maximum load on an arc
- Arc-forwarding index $\overrightarrow{\pi}(\Gamma) = \min_{\mathcal{R}} \overrightarrow{L}(\Gamma, \mathcal{R})$
- Minimal a.f. index $\overrightarrow{\pi}_m(\Gamma)$: same as $\overrightarrow{\pi}(\Gamma)$ but use shortest paths only
- In general,

$$\pi_m(\Gamma) \neq \pi(\Gamma), \overrightarrow{\pi}_m(\Gamma) \neq \overrightarrow{\pi}(\Gamma)$$

$$\pi(\Gamma) \neq 2\overrightarrow{\pi}(\Gamma), \pi_m(\Gamma) \neq 2\overrightarrow{\pi}_m(\Gamma)$$

Trivial lower bounds

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

Equalities $\Leftrightarrow$ there exists an edge-uniform shortest path routing

Trivial lower bounds

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

Equalities $\Leftrightarrow$ there exists an edge-uniform shortest path routing

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

Equalities $\Leftrightarrow$ there exists an arc-uniform shortest path routing

Trivial lower bounds

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

Equalities $\Leftrightarrow$ there exists an edge-uniform shortest path routing

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

Equalities $\Leftrightarrow$ there exists an arc-uniform shortest path routing

Question

A: *Which (non-complete) graphs can achieve these bounds?*

Gossiping

Every vertex has a distinct message to be sent to all other vertices. Carry out this in minimum number of time steps. Define

$$t(\Gamma) = \text{minimum time steps}$$

under the store-and-forward, all-port and full-duplex model:

- a vertex must receive a message wholly before transmitting it to other vertices ('store-and-forward');
- 'all-neighbour transmission' at the same time step ('all-port');
- bidirectional transmission on each edge ('full-duplex');
- it takes one time step to transmit any message over an arc;
- no two messages over the same arc at the same time

A trivial lower bound

For any graph Γ with minimum degree k,

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

A trivial lower bound

For any graph Γ with minimum degree k,

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

Question

B: *Which (non-complete) graphs can achieve this bound?*

Frobenius groups

- A Frobenius group is a non-regular transitive group such that only the identity element can fix two points.
- (Thompson 1959) A finite Frobenius group G on V has a nilpotent normal subgroup K (Frobenius kernel) which is regular on V. Thus

$$G = K.H \text{ (semidirect product)},$$

where H is the stabiliser of a point of V.
- We may think of G as acting on K in such a way that K acts on K by right multiplication and H acts on K by conjugation.

Frobenius graphs

Definition

(Solé 94, Fang-Li-Praeger 98) Let $G = K.H$ be a finite Frobenius group. Call $\mathrm{Cay}(K, S)$ a G-Frobenius graph if

$$S = \begin{cases} a^H, & |H| \text{ even or } |a| = 2 \quad \text{[first-kind]} \\ a^H \cup (a^{-1})^H, & |H| \text{ odd and } |a| \neq 2 \quad \text{[second-kind]} \end{cases}$$

for some $a \in K$ such that $\langle a^H \rangle = K$.

Partial answer

Theorem

(Solé, Fang, Li and Praeger) Let $\Gamma = \mathrm{Cay}(K, S)$ *be a Frobenius graph. Then*

$$\pi(\Gamma) = \frac{\sum_{(u,v)\in V\times V} d(u,v)}{|E|} = \begin{cases} 2\sum_{i=1}^{d} in_i, & \textit{[first-kind]} \\ \sum_{i=1}^{d} in_i, & \textit{[second-kind]} \end{cases}$$

d: diameter of $\mathrm{Cay}(K, S)$
n_i: number of H-orbits of vertices at distance i from 1 in $\mathrm{Cay}(K, S)$, $i = 1, \ldots, d$

Theorem

(Z, 06) Let $\Gamma = \mathrm{Cay}(K, S)$ *be a first-kind Frobenius graph. Then*

$$\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = 2\sum_{i=1}^{d} i n_i$$

and

$$t(\Gamma) = \frac{|K| - 1}{|S|}.$$

Moreover, there exist routing and gossiping schemes with 'nice' properties.

How about second-kind F-graphs?

- From now on we assume $\Gamma = \mathrm{Cay}(K, S)$ is a second-kind Frobenius graph, where

How about second-kind F-graphs?

- From now on we assume $\Gamma = \mathrm{Cay}(K, S)$ is a second-kind Frobenius graph, where
- $G = K.H$ is Frobenius such that $|H|$ is odd, $S = a^H \cup (a^{-1})^H$ for some $a \in K$ with $|a| \neq 2$ and $\langle a^H \rangle = K$.

Gossiping in second-kind F-graphs

Theorem

(Fang and Z, 2010)

$$\frac{|K|-1}{2|H|} \leq t(\Gamma) \leq \frac{|K|-1}{|H|}.$$

If K is abelian, then

$$t(\Gamma) \leq \frac{|K|-1+|I(K)|}{2|H|}$$

where $I(K)$ is the set of involutions of K. In particular, if K is abelian of odd order, then

$$t(\Gamma) = \frac{|K|-1}{2|H|}.$$

Theorem

(cont'd) Moreover, if K is abelian of odd order, then we construct an optimal, shortest-path gossiping scheme for Γ such that the following hold at any time $t = 1, 2, \ldots, (|K| - 1)/2|H|$:

(a) *each arc of Γ is used exactly once for data transmission;*

(b) *for every $x \in K$ exactly $|S|$ arcs are used to transmit messages with source x, and for $t \geq 2$ the set $A_t(x)$ of such arcs is a matching of Γ;*

(c) *K is transitive on the partition $\{A_t(x) : x \in K\}$ of $A(\Gamma)$.*

Remarks

- K is always abelian except when $|H|$ is odd and all Sylow subgroups of H are cyclic.

Remarks

- K is always abelian except when $|H|$ is odd and all Sylow subgroups of H are cyclic.
- The result applies to sharply 2-transitive groups (for them K is always abelian).

Remarks

- K is always abelian except when $|H|$ is odd and all Sylow subgroups of H are cyclic.
- The result applies to sharply 2-transitive groups (for them K is always abelian).
- The proof comes with a gossiping scheme which is optimal when K is abelian of odd order.

Routing in second-kind F-graphs

Theorem

(Fang and Z, 2010) If K is abelian, then there exists a shortest-path routing which is G-edge-transitive, edge-uniform and optimal for $\pi(\Gamma) = \pi_m(\Gamma)$ simultaneously. If in addition $|K|$ is odd, then $\overrightarrow{\pi}(\Gamma) = \overrightarrow{\pi}_m(\Gamma) = \pi(\Gamma)/2$ and this routing is arc-uniform and optimal for $\overrightarrow{\pi}$ and $\overrightarrow{\pi}_m$ as well.

Paley graphs

- Let $q \equiv 1 \pmod 4$ be a prime.

Paley graphs

- Let $q \equiv 1 \pmod 4$ be a prime.
- Paley graph $P(q)$: Cayley graph on $(\mathbb{F}_q, +)$ w.r.t. the set of non-zero squares in $\mathbb{F}_q$, i.e. $x, y \in \mathbb{F}_q$ are adjacent iff $x - y$ is a non-zero square.

Paley graphs

- Let $q \equiv 1 \pmod 4$ be a prime.
- Paley graph $P(q)$: Cayley graph on $(\mathbb{F}_q, +)$ w.r.t. the set of non-zero squares in $\mathbb{F}_q$, i.e. $x, y \in \mathbb{F}_q$ are adjacent iff $x - y$ is a non-zero square.
- $P(q)$ is a Frobenius graph (Solé).

Generalized Paley graphs

- A near field is like a field except that multiplication may not be commutative and there is only a one-sided distributive law.

Generalized Paley graphs

- A near field is like a field except that multiplication may not be commutative and there is only a one-sided distributive law.
- For any near field $(F, +, \cdot)$, we have $(F, +) \cong \mathbb{Z}_p^n$.

Generalized Paley graphs

- A near field is like a field except that multiplication may not be commutative and there is only a one-sided distributive law.
- For any near field $(F, +, \cdot)$, we have $(F, +) \cong \mathbb{Z}_p^n$.

Theorem

Let $(F, +, \cdot)$ be a finite near field of odd order. Let $\beta \in F^*$ and let $H \neq 1$ be a subgroup of $(F^*, \cdot)$ of odd order.

If the left coset βH of H in $(F^*, \cdot)$ is a generating set of $(F, +)$, then $\mathrm{Cay}((F, +), \beta H \cup (-\beta H))$ is a second-kind Frobenius graph.

Corollary

Let $\Gamma = \mathrm{Cay}((F,+), \beta H \cup (-\beta H))$ *be as above. Then*

$$t(\Gamma) = (p^n - 1)/2|H|$$

and there exist optimal gossiping schemes for Γ *such that*

(a) *at any time* t *each arc of* Γ *is used exactly once for data transmission;*

(b) *for each* $x \in K$*, exactly* $2|H|$ *arcs are used to transmit messages with source* x*, and for* $t \geq 2$ *the set* $A_t(x)$ *of such arcs is a matching of* Γ*;*

(c) *the group of translations induced by* $(F,+)$ *is transitive on the partition* $\{A_t(x) : x \in K\}$ *of* $A(\Gamma)$.

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q - 1$ such that either q or $(q - 1)/k$ is even

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q - 1$ such that either q or $(q-1)/k$ is even
- A: subgroup of $(\mathbb{F}_q^*, \cdot)$ of order $(q-1)/k$

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q-1$ such that either q or $(q-1)/k$ is even
- A: subgroup of $(\mathbb{F}_q^*, \cdot)$ of order $(q-1)/k$
- $\mathrm{GPaley}(q, (q-1)/k)$: Cayley graph $\mathrm{Cay}(\mathbb{F}_q, A)$ on $(\mathbb{F}_q, +)$ (Lim and Praeger)

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q - 1$ such that either q or $(q-1)/k$ is even
- A: subgroup of $(\mathbb{F}_q^*, \cdot)$ of order $(q-1)/k$
- $\mathrm{GPaley}(q, (q-1)/k)$: Cayley graph $\mathrm{Cay}(\mathbb{F}_q, A)$ on $(\mathbb{F}_q, +)$ (Lim and Praeger)
- If $q \equiv 1 \pmod 4$, then $\mathrm{GPaley}(q, (q-1)/2) = P(q)$.

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q - 1$ such that either q or $(q - 1)/k$ is even
- A: subgroup of $(\mathbb{F}_q^*, \cdot)$ of order $(q - 1)/k$
- $\mathrm{GPaley}(q, (q - 1)/k)$: Cayley graph $\mathrm{Cay}(\mathbb{F}_q, A)$ on $(\mathbb{F}_q, +)$ (Lim and Praeger)
- If $q \equiv 1 \pmod 4$, then $\mathrm{GPaley}(q, (q - 1)/2) = P(q)$.
- $\mathrm{GPaley}(q, (q - 1)/k)$ is connected iff k is not a multiple of $(q - 1)/(p^m - 1)$ for any proper divisor m of n.

Lim and Praeger's generalized Paley graphs

- $q = p^n$: prime power
- $k \geq 2$: a divisor of $q - 1$ such that either q or $(q-1)/k$ is even
- A: subgroup of $(\mathbb{F}_q^*, \cdot)$ of order $(q-1)/k$
- $\mathrm{GPaley}(q, (q-1)/k)$: Cayley graph $\mathrm{Cay}(\mathbb{F}_q, A)$ on $(\mathbb{F}_q, +)$ (Lim and Praeger)
- If $q \equiv 1 \pmod 4$, then $\mathrm{GPaley}(q, (q-1)/2) = P(q)$.
- $\mathrm{GPaley}(q, (q-1)/k)$ is connected iff k is not a multiple of $(q-1)/(p^m - 1)$ for any proper divisor m of n.
- If q is odd and $\mathrm{GPaley}(q, (q-1)/k)$ is connected, then $\mathrm{GPaley}(q, (q-1)/k)$ is the second-kind Frobenius graph $\mathrm{Cay}((\mathbb{F}_q, +), 1A \cup (-1A))$.

Corollary

For connected Lim-Praeger graphs $\mathrm{GPaley}(q,(q-1)/k)$*, we have*

$$t(\mathrm{GPaley}(q,(q-1)/k)) = k$$

and there exists an optimal gossiping scheme having properties (a)-(c) in the previous corollary.

An example

- 3 is a primitive element of $\mathbb{F}_{19}$

An example

- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)

An example

- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)
- $3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$ is a generating set of $(\mathbb{F}_{19}, +)$

An example

- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)
- $3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$ is a generating set of $(\mathbb{F}_{19}, +)$
- $3H \cup (-3H) = \{2, 14, 3, 17, 5, 16\}$

An example

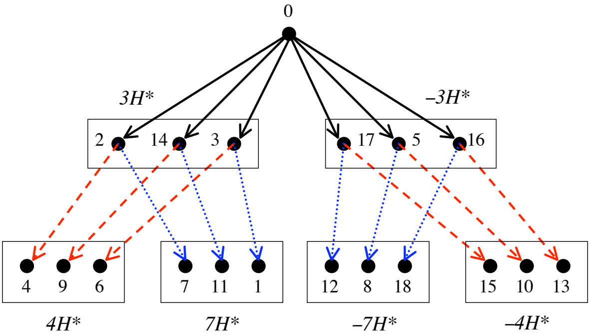
- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)
- $3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$ is a generating set of $(\mathbb{F}_{19}, +)$
- $3H \cup (-3H) = \{2, 14, 3, 17, 5, 16\}$
- $\Gamma = \mathrm{Cay}(\mathbb{Z}_{19}, \{2, 14, 3, 17, 5, 16\})$ is a second-kind $\mathbb{Z}_{19}.\mathbb{Z}_3$-Frobenius graph (not a Lim-Praeger graph)

An example

- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)
- $3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$ is a generating set of $(\mathbb{F}_{19}, +)$
- $3H \cup (-3H) = \{2, 14, 3, 17, 5, 16\}$
- $\Gamma = \mathrm{Cay}(\mathbb{Z}_{19}, \{2, 14, 3, 17, 5, 16\})$ is a second-kind $\mathbb{Z}_{19}.\mathbb{Z}_3$-Frobenius graph (not a Lim-Praeger graph)
- $\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = 1 \cdot 2 + 2 \cdot 4 = 10$

An example

- 3 is a primitive element of $\mathbb{F}_{19}$
- $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\}$ (unique subgroup of $\mathbb{F}_{19}^*$ of order 3)
- $3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$ is a generating set of $(\mathbb{F}_{19}, +)$
- $3H \cup (-3H) = \{2, 14, 3, 17, 5, 16\}$
- $\Gamma = \mathrm{Cay}(\mathbb{Z}_{19}, \{2, 14, 3, 17, 5, 16\})$ is a second-kind $\mathbb{Z}_{19}.\mathbb{Z}_3$-Frobenius graph (not a Lim-Praeger graph)
- $\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = 1 \cdot 2 + 2 \cdot 4 = 10$
- $t(\Gamma) = (19 - 1)/(2 \cdot 3) = 3$



A routing and gossiping tree for $\mathrm{Cay}(\mathbb{Z}_{19}, \{2, 14, 3, 17, 5, 16\})$ at root 0.

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Corollary

For any even integer $r \geq 4$, there exist infinitely many odd primes p such that there is a second-kind Frobenius graph (connected generalized Paley graph) of order p^2 and valency r with the kernel of the underlying Frobenius group abelian.

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Corollary

For any even integer $r \geq 4$, there exist infinitely many odd primes p such that there is a second-kind Frobenius graph (connected generalized Paley graph) of order p^2 and valency r with the kernel of the underlying Frobenius group abelian.

Proof: Dirichlet theorem: $\exists$ infinitely many primes in

$$-1 + r, -1 + 2r, -1 + 3r, \ldots$$

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Corollary

For any even integer $r \geq 4$, there exist infinitely many odd primes p such that there is a second-kind Frobenius graph (connected generalized Paley graph) of order p^2 and valency r with the kernel of the underlying Frobenius group abelian.

Proof: Dirichlet theorem: $\exists$ infinitely many primes in

$$-1 + r, -1 + 2r, -1 + 3r, \ldots$$

Let $p = -1 + tr$ be such an odd prime, $k = t(p-1)$ and $q = p^2$.

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Corollary

For any even integer $r \geq 4$, there exist infinitely many odd primes p such that there is a second-kind Frobenius graph (connected generalized Paley graph) of order p^2 and valency r with the kernel of the underlying Frobenius group abelian.

Proof: Dirichlet theorem: $\exists$ infinitely many primes in

$$-1 + r, -1 + 2r, -1 + 3r, \ldots$$

Let $p = -1 + tr$ be such an odd prime, $k = t(p-1)$ and $q = p^2$. Then $r = (q-1)/k$ and r is not a divisor of $p - 1$.

Second-kind F-graphs with small valency and large order

Question

Are there 'large' second-kind F-graphs with 'small' valency?

Corollary

For any even integer $r \geq 4$, there exist infinitely many odd primes p such that there is a second-kind Frobenius graph (connected generalized Paley graph) of order p^2 and valency r with the kernel of the underlying Frobenius group abelian.

Proof: Dirichlet theorem: $\exists$ infinitely many primes in

$$-1 + r, -1 + 2r, -1 + 3r, \ldots$$

Let $p = -1 + tr$ be such an odd prime, $k = t(p-1)$ and $q = p^2$.
Then $r = (q-1)/k$ and r is not a divisor of $p - 1$.
$\mathrm{GPaley}(p^2, r)$ is a second-kind Frobenius graph of order p^2 and valency r whose underlying Frobenius group has an abelian kernel.

Summary: second-kind Frobenius graphs

Properties	**Any** $K.H$	K **abelian**	K **abelian & $\|K\|$ odd**
Hamiltonian?	Conjecture	Yes M	Yes M
π	Best possible FLP	?	?
π_m	Best possible FLP	?	?
Optimal routing for π and π_m?	Unknown	FZ	FZ
$\overrightarrow{\pi}$	Unknown	Unknown	Best possible FZ
$\overrightarrow{\pi}_m$	Unknown	Unknown	Best possible FZ
Optimal routing for $\overrightarrow{\pi}$ and $\overrightarrow{\pi}_m$?	Unknown	Unknown	FZ
Gossiping time	$\leq 2\cdot$(trivial bound)	–	Best possible FZ
Gossiping algorithm	2-Factor approximation FZ	–	Exact algorithm Nice properties FZ