Recent progress on Frobenius graphs and related topics

Sanming Zhou

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

IWONT 2011, Brussels

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:
  - Degree/diameter problem
  - Expandability, etc.

Motivation

- **Question**: Which network topologies can assure high performance?
- Answer depends on how we measure performance:
  - Degree/diameter problem
  - Expandability, etc.
- We consider two measures:
  - minimum gossiping time
  - minimum edge-congestion for all-to-all routing

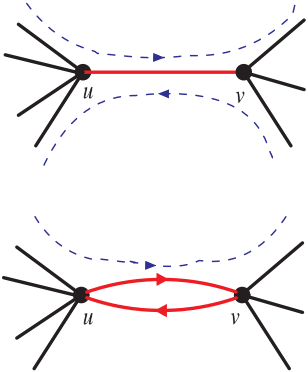
Motivation

- **Question**: Which network topologies can assure high performance?
- Answer depends on how we measure performance:
  - Degree/diameter problem
  - Expandability, etc.
- We consider two measures:
  - minimum gossiping time
  - minimum edge-congestion for all-to-all routing
- What are the 'most efficient' graphs (of small degree) 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


u
v
u
v

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 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.

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

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 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 to Question A

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

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

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

Theorem

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

(a) *a shortest path routing;*

(b) G*-arc transitive;*

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

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

Moreover, if the H*-orbits on* K *are known, we can construct such routings (not unique) in polynomial time. Furthermore, we have*

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

The formula for $\overrightarrow{\pi}_m$ and a result of Diaconis-Stroock imply:

Corollary

Let Γ, d, n_i be as above. Then

$$\lambda_2(\Gamma) \leq |H| - \frac{|K|}{d\sum_{i=1}^{d} in_i}.$$

Partial answer to Question B

Theorem

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

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

Moreover, there exist optimal gossiping schemes such that

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

(b) *at any time every arc is used exactly once;*

(c) *at any time ≥ 2 and for any vertex g, the set $A(g)$ of arcs transmitting the message originated from g is a matching of Γ, and $\{A(g) : g \in K\}$ is a partition of the arcs of Γ.*

Furthermore, if we know the H-orbits on K, then we can construct such schemes (not unique) in polynomial time.

Two families of first-kind Frobenius graphs

'Double-loop' network $DL_n(a, b)$:
Vertex set $\mathbb{Z}_n$, $x \sim x \pm a, x \sim x \pm b \pmod{n}$, where $n \geq 5, 1 \leq a \neq b \leq n-1, a, b \neq n/2, a+b \neq n$.

'Triple-loop' network $TL_n(a, b, 1)$: Similar

Theorem

(Thomson and Z, 08) If $n \geq 6$ is even, then there exists no first kind Frobenius circulant graph of order n and valency four. If $n = p_1^{e_1} \cdots p_l^{e_l} \geq 5$ is odd, the following are equivalent:

(a) *$\exists h$ such that $DL_n(1, h)$ is a first kind Frobenius graph;*

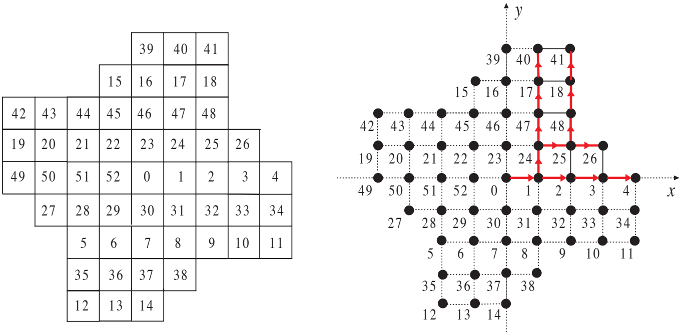
(b) *$x^2 + 1 \equiv 0 \mod n$ has a solution;*

(c) *$p_i \equiv 1 \mod 4$ for each i.*

Moreover, if one of these holds, then

(d) *each solution h to $x^2 + 1 \equiv 0$ mod n gives rise to a first kind Frobenius $DL_n(1, h)$, and vice versa;*

(e) *there are exactly 2^{l-1} pairwise non-isomorphic 4-valent first kind Frobenius circulant graphs with order n, and each of them is isomorphic to some $DL_n(1, h)$.*



(a) (b)

Optimal gossiping and routing in $DL_{53}(1, 23)$.

Corollary

Let $\Gamma = DL_{n_d}(1, 2d+1)$ *be the unique connected 4-valent circulant graph of diameter* $d \geq 2$ *and maximum order* $n_d = 2d^2 + 2d + 1$ *(Yebra-Fiol-Morillo-Alegre).*

Then Γ *is a* $\mathbb{Z}_{n_d}.H(d)$*-Frobenius graph, where*

$$H(d) = \{[1], [2d+1], -[1], -[2d+1]\}.$$

Moreover,

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

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

Theorem

(Thomson and Z, 09–10) There exists a 6-valent first kind Frobenius circulant $TL_n(a, b, 1)$ *of order* $n = p_1^{e_1} \cdots p_l^{e_l} \geq 7$ *if and only if* $n \equiv 1 \mod 6$ *and*

$$x^2 - x + 1 \equiv 0 \mod n$$

has a solution. Moreover, if these conditions hold, then

(a) *each solution a to the equation above gives rise to a first kind Frobenius* $TL_n(a, b, 1)$*, and vice versa, and in this case* $b \equiv a - 1 \mod n$*;*

(b) *there are exactly* 2^{l-1} *pairwise non-isomorphic 6-valent first kind Frobenius circulants of order n, and each of them is isomorphic to some* $TL_n(a, a - 1, 1)$*.*

Corollary

The unique connected 6-valent circulant graph $TL_{n_d}(3d+1, 1, -(3d+2))$ of diameter $d \geq 2$ and maximum order $n_d = 3d^2 + 3d + 1$ (Yebra-Fiol-Morillo-Alegre) is a first kind Frobenius graph.
Moreover,

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

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

Broadcasting time

Theorem

(a) (Z, 10) The broadcasting time of a Frobenius $DL_n(1, h)$ *is equal to* $diam(DL_n(1, h)) + 2$*.*

(b) (Thomson and Z, 09–10) The broadcasting time of a Frobenius $TL_n(a, a-1, 1)$ *is equal to* $diam(DL_n(1, h)) + 2$ *or* $diam(DL_n(1, h)) + 3$*, and both cases can occur.*

Gaussian graphs

Definition

(Martínez, Beivide and Gabidulin 07) Let

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

$$\mathbb{Z}[i]_\alpha = \mathbb{Z}[i]/(\alpha),\ 0 \neq \alpha = a + bi,\ \gcd(a, b) = 1$$

$$d_\alpha([\beta]_\alpha, [\gamma]_\alpha) = \min\{|x| + |y| : [\beta - \gamma]_\alpha = [x + yi]_\alpha\}$$

The Gaussian graph G_α is defined to have vertex set $\mathbb{Z}[i]_\alpha$ such that $[\beta]_\alpha \sim [\gamma]_\alpha$ iff $d_\alpha([\beta]_\alpha, [\gamma]_\alpha) = 1$.

Thus

$$G_\alpha = \mathrm{Cay}((\mathbb{Z}[i]_\alpha, +), H_\alpha)$$

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

Lemma

(Z, 10) When the norm $N(\alpha) = a^2 + b^2$ is odd, G_α is a 4-valent Frobenius circulant, and vice versa.

Theorem

(MBG 07; Thomson for odd $N(\alpha)$) Suppose $0 < a < b$ in $\alpha = a + bi$ w.l.o.g. Then

$$diam(G_\alpha) = \begin{cases} b, & \text{if } N(\alpha) \text{ is even} \\ b-1, & \text{if } N(\alpha) \text{ is odd.} \end{cases}$$

Eisenstein-Jacobi graphs

Definition

(Martínez, Beivide and Gabidulin 07) Let

$$\rho = (1 + \sqrt{3}i)/2$$

$$\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$$

$$\alpha = c + d\rho \in \mathbb{Z}[\rho], \ \ \mathtt{gcd}(c, d) = 1, \ \ N(\alpha) = c^2 + cd + d^2 \geq 5$$

The EJ-graph EJ_α is defined as the Cayley graph on $(\mathbb{Z}[\rho]_\alpha, +)$ with respect to $\{\pm[1]_\alpha, \pm[\rho]_\alpha, \pm[\rho^2]_\alpha\}$.

Lemma

(Z, 10) The Frobenius circulant $TL_n(a, a-1, 1)$ is an EJ-graph.

Theorem

(Flahive and Bose 10) Suppose $a \geq b \geq 0$ w.l.o.g. Then

$$diam(EJ_\alpha) = \frac{2a+b}{3}.$$

How about second-kind F-graphs?

Let

$$\Gamma = \mathrm{Cay}(K, S)$$

be 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 $\langle a^H \rangle = K$.

Theorem

(Fang and Z, 10) When K is abelian of odd order, Γ admits 'perfect' routing and gossiping schemes.
Otherwise, we only obtain an upper bound on the gossiping time and a 2-factor approximation algorithm.

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

Paley graphs

Definition

Let $q \equiv 1 \pmod 4$ be a prime. The Paley graph $P(q)$ is the Cayley graph on $(\mathbb{F}_q, +)$ w.r.t. the set of non-zero squares in $\mathbb{F}_q$.

$P(q)$ is a Frobenius graph (Solé).

Near fields

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

A field is a near field, but the converse is not true.

For any near field $(F, +, \cdot)$, $(F, +)$ is an elementary abelian group $\mathbb{Z}_p^n$. In particular, $|F| = p^n$ is a prime power.

Generalized generalized Paley graphs

Theorem

(Fang and Z, 10) 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.*

Generalized Paley graphs

Definition

(Lim and Praeger 09) Let $q = p^n$ and $k \geq 2$ be a divisor of $q - 1$ such that either q or $(q-1)/k$ is even. Let $A \leq (\mathbb{F}_q^*, \cdot)$ with order $(q-1)/k$. Define

$$\mathrm{GPaley}(q, (q-1)/k) = \mathrm{Cay}((\mathbb{F}_q, +), A).$$

If $q \equiv 1 \pmod 4$, then $\mathrm{GPaley}(q, (q-1)/2) = P(q)$.

If q is odd and $\mathrm{GPaley}(q, (q-1)/k)$ is connected, then

$$\mathrm{GPaley}(q, (q-1)/k) \cong \mathrm{Cay}((\mathbb{F}_q, +), 1A \cup (-1A))$$

which is a second-kind Frobenius graph. (Lim and Praeger: We know exactly when $\mathrm{GPaley}(q, (q-1)/k)$ is connected.)

Corollary

(Fang and Z, 10) Let $\Gamma = \mathrm{Cay}((F,+), \beta H \cup (-\beta H))$ *be as before. 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 when* $t \geq 2$ *the set* $A_t(x)$ *of such arcs form a matching of* Γ*.*

In particular,

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

and (a)-(b) hold for $\mathrm{GPaley}(q, (q-1)/k)$*.*

An example

Let $H = \langle 3^6 \rangle = \{3^6 = 7, 3^{12} = 11, 3^{18} = 1\} \leq \mathbb{F}_{19}^*$ (3 is a primitive element of $\mathbb{F}_{19}$). Then

$$3H = \{7 \cdot 3 = 2, 11 \cdot 3 = 14, 3\}$$

is a generating set of $(\mathbb{F}_{19}, +)$. So

$$\Gamma = \mathrm{Cay}(\mathbb{Z}_{19}, 3H \cup (-3H)) = \mathrm{Cay}(\mathbb{Z}_{19}, \{2, 14, 3, 17, 5, 16\})$$

is a second-kind $\mathbb{Z}_{19}.\mathbb{Z}_3$-Frobenius graph (but not a Lim-Praeger graph).

$$\pi(\Gamma) = 2\overrightarrow{\pi}(\Gamma) = 2\overrightarrow{\pi}_m(\Gamma) = \pi_m(\Gamma) = 1 \cdot 2 + 2 \cdot 4 = 10$$
$$t(\Gamma) = (19-1)/(2 \cdot 3) = 3$$

Finally ... degree-diameter ...

Finally ... degree-diameter ...

Proposition

(a) *For any even integer* $\Delta \geq 2$,

$$N^{at}(\Delta, 2) \geq \frac{1}{4}(\Delta + 2)^2.$$

(b) *For any* $0 < \varepsilon < 1$, *there exist infinitely many odd integers* Δ *of the form* $q^3(q^{d-2} - 1)/(q - 1)$, *where* q *is an odd prime power and* $d \geq 3/\varepsilon$ *is an odd integer, such that*

$$N^{at}(\Delta, 2) > \Delta^{2-\varepsilon} + 2\Delta^{1-\frac{\varepsilon}{3}} + \Delta^{1-\frac{2\varepsilon}{3}} + 3.$$

Finally ... degree-diameter ...

Proposition

(a) *For any even integer* $\Delta \geq 2$,

$$N^{at}(\Delta, 2) \geq \frac{1}{4}(\Delta + 2)^2.$$

(b) *For any* $0 < \varepsilon < 1$, *there exist infinitely many odd integers* Δ *of the form* $q^3(q^{d-2} - 1)/(q - 1)$, *where* q *is an odd prime power and* $d \geq 3/\varepsilon$ *is an odd integer, such that*

$$N^{at}(\Delta, 2) > \Delta^{2-\varepsilon} + 2\Delta^{1-\frac{\varepsilon}{3}} + \Delta^{1-\frac{2\varepsilon}{3}} + 3.$$

Question

Are there infinitely many integers $\Delta \geq 2$ *such that*

$$N^{at}(\Delta, 2) \geq \Delta^2 - f(\Delta)$$

for some function f *with* $f(x)/x^2 \to 0$ *as* $x \to \infty$?