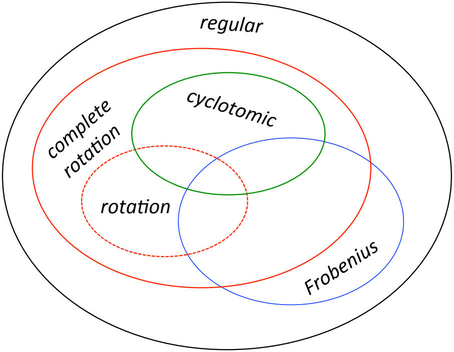
Constructing Cayley graphs for efficient data transmission

Sanming Zhou

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

IWONT 2014, Bratislava, 30/6–4/7/2014

Graphs to be discussed



A few classes of Cayley graphs $\mathrm{Cay}(K, S)$ defined in terms of $\mathrm{Aut}(K, S)$ (setwise stabiliser of S in $\mathrm{Aut}(K)$)

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Outline

- Motivation
- Frobenius graphs
- 6-valent first-kind Frobenius circulants and Eisenstein-Jacobi networks
- Rotational circulants
- FFCs of valency $2p$ or $2p^2$
- Cyclotomic graphs

Motivation

Question

What network topologies enable efficient data transmission?

- Measure of efficiency
  - transmission time (e.g. gossiping time, broadcasting time)
  - congestion on edges/arcs/vertices
  - etc.
- What are the 'most efficient' graphs (of small degree) with respect to these measures?

Motivation

Question

What network topologies enable efficient data transmission?

- Measure of efficiency
    - transmission time (e.g. gossiping time, broadcasting time)
    - congestion on edges/arcs/vertices
    - etc.
- What are the 'most efficient' graphs (of small degree) with respect to these measures?

Routing

Design a data transmission route (oriented path) for each ordered pair of vertices.

- A set of such oriented paths is called an all-to-all **routing**
- **Load of an edge** = number of paths traversing the edge in either direction
- An **arc** is an oriented edge
- **Load of an arc** = number of paths traversing the arc in its direction

Routing

Design a data transmission route (oriented path) for each ordered pair of vertices.

- A set of such oriented paths is called an all-to-all **routing**
- **Load of an edge** = number of paths traversing the edge in either direction
- An **arc** is an oriented edge
- **Load of an arc** = number of paths traversing the arc in its direction

Routing

Design a data transmission route (oriented path) for each ordered pair of vertices.

- A set of such oriented paths is called an all-to-all **routing**
- **Load of an edge** = number of paths traversing the edge in either direction
- An **arc** is an oriented edge
- **Load of an arc** = number of paths traversing the arc in its direction

Routing

Design a data transmission route (oriented path) for each ordered pair of vertices.

- A set of such oriented paths is called an all-to-all **routing**
- **Load of an edge** = number of paths traversing the edge in either direction
- An **arc** is an oriented edge
- **Load of an arc** = number of paths traversing the arc in its direction

Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load of an edge under routing $\mathcal{R}$
- $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$ (**edge-forwarding index**)
- $\pi_m(\Gamma)$: use shortest paths only (**minimal e.f.i.**)
- $\overrightarrow{\pi}(\Gamma)$ (**arc-forwarding index**)
- $\overrightarrow{\pi}_m(\Gamma)$: use shortest paths only (**minimal a.f.i.**)

Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load of an edge under routing $\mathcal{R}$
- $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$ (**edge-forwarding index**)
- $\pi_m(\Gamma)$: use shortest paths only (**minimal e.f.i.**)
- $\overrightarrow{\pi}(\Gamma)$ (**arc-forwarding index**)
- $\overrightarrow{\pi}_m(\Gamma)$: use shortest paths only (**minimal a.f.i.**)

Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load of an edge under routing $\mathcal{R}$
- $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$ (**edge-forwarding index**)
- $\pi_m(\Gamma)$: use shortest paths only (**minimal e.f.i.**)
- $\overrightarrow{\pi}(\Gamma)$ (**arc-forwarding index**)
- $\overrightarrow{\pi}_m(\Gamma)$: use shortest paths only (**minimal a.f.i.**)

Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load of an edge under routing $\mathcal{R}$
- $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$ (**edge-forwarding index**)
- $\pi_m(\Gamma)$: use shortest paths only (**minimal e.f.i.**)
- $\overrightarrow{\pi}(\Gamma)$ (**arc-forwarding index**)
- $\overrightarrow{\pi}_m(\Gamma)$: use shortest paths only (**minimal a.f.i.**)

Edge- and arc-forwarding indices

- $L(\Gamma, \mathcal{R})$ = maximum load of an edge under routing $\mathcal{R}$
- $\pi(\Gamma) = \min_{\mathcal{R}} L(\Gamma, \mathcal{R})$ (**edge-forwarding index**)
- $\pi_m(\Gamma)$: use shortest paths only (**minimal e.f.i.**)
- $\overrightarrow{\pi}(\Gamma)$ (**arc-forwarding index**)
- $\overrightarrow{\pi}_m(\Gamma)$: use shortest paths only (**minimal a.f.i.**)

Trivial lower bounds

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

Equality **iff** there exists an **edge-uniform shortest path routing**

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

Equality **iff** there exists an **arc-uniform shortest path routing**

Question

I: *Which graphs can achieve these bounds?*

Trivial lower bounds

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

Equality **iff** there exists an **edge-uniform shortest path routing**

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

Equality **iff** there exists an **arc-uniform shortest path routing**

Question

I: *Which graphs can achieve these bounds?*

Trivial lower bounds

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

Equality **iff** there exists an **edge-uniform shortest path routing**

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

Equality **iff** there exists an **arc-uniform shortest path routing**

Question

I: *Which graphs can achieve these bounds?*

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping

In least number of time steps, transmit a distinct message at each vertex to all other vertices:

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

Gossiping time

Definition

Gossiping time of a graph $\Gamma = (V, E)$:

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

A trivial bound:

$$t(\Gamma) \geqslant \left\lceil \frac{n-1}{\delta} \right\rceil,$$

where n is the order and δ the minimum degree of Γ

Question

II: *Which graphs can achieve this bound?*

Gossiping time

Definition

Gossiping time of a graph $\Gamma = (V, E)$:

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

A trivial bound:

$$t(\Gamma) \geqslant \left\lceil \frac{n-1}{\delta} \right\rceil,$$

where n is the order and δ the minimum degree of Γ

Question

II: *Which graphs can achieve this bound?*

Gossiping time

Definition

Gossiping time of a graph $\Gamma = (V, E)$:

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

A trivial bound:

$$t(\Gamma) \geqslant \left\lceil \frac{n-1}{\delta} \right\rceil,$$

where n is the order and δ the minimum degree of Γ

Question

II: *Which graphs can achieve this bound?*

Broadcasting

In least number of time steps, transmit a message from a specific source vertex to all other vertices:

- at each time step, any vertex who has got the message already can retransmit it to **at most one** of its neighbours
- one time step to transmit over an arc

Definition

For every $u \in V$, define

$$b(\Gamma, u) = \text{minimum time steps if } u \text{ is the source vertex}$$

Broadcasting time of Γ:

$$b(\Gamma) = \max_u b(\Gamma, u)$$

Broadcasting

In least number of time steps, transmit a message from a specific source vertex to all other vertices:

- at each time step, any vertex who has got the message already can retransmit it to **at most one** of its neighbours
- one time step to transmit over an arc

Definition

For every $u \in V$, define

$$b(\Gamma, u) = \text{minimum time steps if } u \text{ is the source vertex}$$

Broadcasting time of Γ:

$$b(\Gamma) = \max_{u} b(\Gamma, u)$$

Semidirect product

Definition

Let H and K be groups such that H acts on K as a group. That is, there is a homomorphism $H \to \mathrm{Aut}(K)$.

The **semidirect product** of K by H, $K.H$, is the group on $K \times H$ under the operation:

$$(k_1, h_1)(k_2, h_2) := (k_1 k_2^{h_1^{-1}}, h_1 h_2).$$

Equivalently, $G = K.H$ if

$$K \trianglelefteq G, H \leqslant G, G = HK, H \cap K = 1.$$

Semidirect product

Definition

Let H and K be groups such that H acts on K as a group. That is, there is a homomorphism $H \to \mathrm{Aut}(K)$.

The **semidirect product** of K by H, $K.H$, is the group on $K \times H$ under the operation:

$$(k_1, h_1)(k_2, h_2) := (k_1 k_2^{h_1^{-1}}, h_1 h_2).$$

Equivalently, $G = K.H$ if

$$K \trianglelefteq G, H \leqslant G, G = HK, H \cap K = 1.$$

Semidirect product

Definition

Let H and K be groups such that H acts on K as a group. That is, there is a homomorphism $H \to \mathrm{Aut}(K)$.

The **semidirect product** of K by H, $K.H$, is the group on $K \times H$ under the operation:

$$(k_1, h_1)(k_2, h_2) := (k_1 k_2^{h_1^{-1}}, h_1 h_2).$$

Equivalently, $G = K.H$ if

$$K \trianglelefteq G, H \leqslant G, G = HK, H \cap K = 1.$$

Frobenius groups

Definition

A **Frobenius group** is a transitive group such that

- there exist non-identity elements fixing one point
- only the identity element can fix two points

Theorem

(Thompson 1959)
*A finite Frobenius group G on V has a nilpotent normal subgroup K (**Frobenius kernel**) which is regular on V. Thus*

$$G = K.H$$

where H is the stabiliser of a point of V.

We may identify V with K such that K acts on itself by right multiplication and H (stabiliser of 1) acts on K by conjugation.

Frobenius groups

Definition

A **Frobenius group** is a transitive group such that

- there exist non-identity elements fixing one point
- only the identity element can fix two points

Theorem

(Thompson 1959)
*A finite Frobenius group G on V has a nilpotent normal subgroup K (**Frobenius kernel**) which is regular on V. Thus*

$$G = K.H$$

where H is the stabiliser of a point of V.

We may identify V with K such that K acts on itself by right multiplication and H (stabiliser of 1) acts on K by conjugation.

Frobenius groups

Definition

A **Frobenius group** is a transitive group such that

- there exist non-identity elements fixing one point
- only the identity element can fix two points

Theorem

(Thompson 1959)
*A finite Frobenius group G on V has a nilpotent normal subgroup K (**Frobenius kernel**) which is regular on V. Thus*

$$G = K.H$$

where H is the stabiliser of a point of V.

We may identify V with K such that K acts on itself by right multiplication and H (stabiliser of 1) acts on K by conjugation.

First-kind Frobenius graphs

Definition

(Solé 1994, Fang-Li-Praeger 1998)
Let $G = K.H$ be a finite Frobenius group.

Let $a \in K$ and let

$$a^H := \{h^{-1}ah : h \in H\}$$

be the H-orbit on K containing a.

Suppose $\langle a^H \rangle = K$ and $|H|$ is even or $|a| = 2$.

Call

$$\mathrm{Cay}(K, a^H)$$

a **first-kind** G**-Frobenius graph**.

First-kind Frobenius graphs

Definition

(Solé 1994, Fang-Li-Praeger 1998)
Let $G = K.H$ be a finite Frobenius group.

Let $a \in K$ and let

$$a^H := \{h^{-1}ah : h \in H\}$$

be the H-orbit on K containing a.

Suppose $\langle a^H \rangle = K$ and $|H|$ is even or $|a| = 2$.

Call

$$\mathrm{Cay}(K, a^H)$$

a **first-kind G-Frobenius graph**.

First-kind Frobenius graphs

Definition

(Solé 1994, Fang-Li-Praeger 1998)
Let $G = K.H$ be a finite Frobenius group.

Let $a \in K$ and let

$$a^H := \{h^{-1}ah : h \in H\}$$

be the H-orbit on K containing a.

Suppose $\langle a^H \rangle = K$ and $|H|$ is even or $|a| = 2$.

Call

$$\mathrm{Cay}(K, a^H)$$

a **first-kind** G**-Frobenius graph**.

First-kind Frobenius graphs

Definition

(Solé 1994, Fang-Li-Praeger 1998)
Let $G = K.H$ be a finite Frobenius group.

Let $a \in K$ and let

$$a^H := \{h^{-1}ah : h \in H\}$$

be the H-orbit on K containing a.

Suppose $\langle a^H \rangle = K$ and $|H|$ is even or $|a| = 2$.

Call

$$\mathrm{Cay}(K, a^H)$$

a **first-kind G-Frobenius graph**.

Partial answer to Question I

Theorem

(Solé 1994, Fang-Li-Praeger 1998)
Let Γ be a (first- or second-kind) G-Frobenius graph. Then

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

Theorem

(Zhou 2009)
Let Γ be a **first-kind** *G-Frobenius graph, where $G = K.H$. 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 a routing in polynomial time. Furthermore, we have

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

An algorithm for producing many routings with the properties above was given.

Theorem

(Zhou 2009)
*Let Γ be a **first-kind** G-Frobenius graph, where $G = K.H$. 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, $\vec{\pi}$, $\vec{\pi}_m$, π_m simultaneously.*

Moreover, if the H-orbits on K are known, we can construct such a routing in polynomial time. Furthermore, we have

$$\pi(\Gamma) = 2\vec{\pi}(\Gamma) = 2\vec{\pi}_m(\Gamma) = \pi_m(\Gamma)$$

An algorithm for producing many routings with the properties above was given.

Theorem

(Zhou 2009)

Let Γ be a **first-kind** *G-Frobenius graph, where $G = K.H$. 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 a routing in polynomial time. Furthermore, we have

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

An algorithm for producing many routings with the properties above was given.

Partial answer to Question II

Theorem

(Zhou 2009)
Let Γ be a **first-kind** *G-Frobenius graph, where $G = K.H$. 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 for message transmission;*

(c) *at any time $\geqslant 2$ 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 in polynomial time.

Remarks

- In theory, first-kind Frobenius graphs are ‘perfect’ as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are 'perfect' as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are 'perfect' as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are ‘perfect’ as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are ‘perfect’ as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are 'perfect' as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

Remarks

- In theory, first-kind Frobenius graphs are ‘perfect’ as far as routing and gossiping are concerned
- This is part of a more general framework
- Second-kind Frobenius graphs are also good but not as good as first-kind Frobenius graphs for gossiping
- It is desirable to construct concrete families of first-kind Frobenius graphs of small valency
- **FFC**: first-kind Frobenius circulant
- Classification of 4-valent FFCs (Thomson and Zhou 2008)
- Classification of 6-valent FFCs (Thomson and Zhou 2008-2014)

6-valent circulants

- Circulant graph:

$$C(n, S) := \mathrm{Cay}(\mathbb{Z}_n, S)$$

  where $-S = S \subseteq \mathbb{Z}_n \backslash \{0\}$
- Triple-loop network:

$$TL_n(a, b, c) := C(n, \{\pm a, \pm b, \pm c\})$$

  where $n \geqslant 7$ and $1 \leqslant a, b, c \leqslant n - 1$ such that $a, b, c, n-a, n-b, n-c$ are pairwise distinct
- We consider $TL_n(a, b, 1)$ only

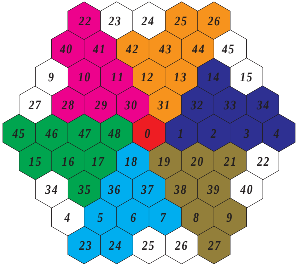
Geometric triple-loop network

Definition

(Yebra, Fiol, Morillo and Alegre 85) $TL_n(a,b,c)$ is **geometric** if

$$a' + b' + c' \equiv 0 \mod n$$

for some $a' \in \{a, n-a\}, b' \in \{b, n-b\}, c' \in \{c, n-c\}$.



Hexagonal tessellation of $TL_{49}(31, 1, 30)$

Rotational Cayley graphs

Definition

(Bermond, Kodate and Pérennes 1996)
A **complete rotation** of $\mathrm{Cay}(K, S)$ is an automorphism of K that induces a cyclic permutation on S.

$\mathrm{Cay}(K, S)$ is **rotational** if it admits a complete rotation.

(Fragopoulou, Akl and Meijer 1996)
A **rotation** of $\mathrm{Cay}(K, S)$ is an inner automorphism of K that induces a cyclic permutation on S.

For example, $H(d, q)$ is rotational when q is a prime power.

Rotational Cayley graphs

Definition

(Bermond, Kodate and Pérennes 1996)
A **complete rotation** of $\mathrm{Cay}(K, S)$ is an automorphism of K that induces a cyclic permutation on S.

$\mathrm{Cay}(K, S)$ is **rotational** if it admits a complete rotation.

(Fragopoulou, Akl and Meijer 1996)
A **rotation** of $\mathrm{Cay}(K, S)$ is an inner automorphism of K that induces a cyclic permutation on S.

For example, $H(d, q)$ is rotational when q is a prime power.

Rotational Cayley graphs

Definition

(Bermond, Kodate and Pérennes 1996)
A **complete rotation** of $\mathrm{Cay}(K, S)$ is an automorphism of K that induces a cyclic permutation on S.

$\mathrm{Cay}(K, S)$ is **rotational** if it admits a complete rotation.

(Fragopoulou, Akl and Meijer 1996)
A **rotation** of $\mathrm{Cay}(K, S)$ is an inner automorphism of K that induces a cyclic permutation on S.

For example, $H(d, q)$ is rotational when q is a prime power.

Rotational Cayley graphs

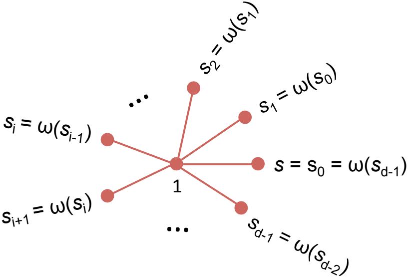
Definition

(Bermond, Kodate and Pérennes 1996)
A **complete rotation** of $\mathrm{Cay}(K, S)$ is an automorphism of K that induces a cyclic permutation on S.

$\mathrm{Cay}(K, S)$ is **rotational** if it admits a complete rotation.

(Fragopoulou, Akl and Meijer 1996)
A **rotation** of $\mathrm{Cay}(K, S)$ is an inner automorphism of K that induces a cyclic permutation on S.

For example, $H(d, q)$ is rotational when q is a prime power.



A complete rotation ω of Cay(K, S):

$$S = s^{\langle \omega \rangle} = \{s, s^{\omega}, \ldots, s^{\omega^{d-1}}\}$$

Rotational Cayley graphs v.s. balanced regular Cayley maps

Definition

A cyclic permutation ρ of S induces a natural embedding of $\mathrm{Cay}(G, S)$, giving a **Cayley map** $M = CM(G, S, \rho)$.

(Škoviera and Širáň 1992) M is **balanced** if $\rho(s^{-1}) = \rho(s)^{-1}$ for $s \in S$, and **regular** if $\mathrm{Aut}(M)$ is regular on the set of arcs of $\mathrm{Cay}(G, S)$.

A complete rotation in a Cayley graph $\Leftrightarrow$ a 2-cell embedding on a closed orientable surface as a balanced regular Cayley map

Rotational Cayley graphs v.s. balanced regular Cayley maps

Definition

A cyclic permutation ρ of S induces a natural embedding of $\mathrm{Cay}(G, S)$, giving a **Cayley map** $M = CM(G, S, \rho)$.

(Škoviera and Širáň 1992) M is **balanced** if $\rho(s^{-1}) = \rho(s)^{-1}$ for $s \in S$, and **regular** if $\mathrm{Aut}(M)$ is regular on the set of arcs of $\mathrm{Cay}(G, S)$.

A complete rotation in a Cayley graph $\Leftrightarrow$ a 2-cell embedding on a closed orientable surface as a balanced regular Cayley map

Theorem

(Thomson and Zhou 2008-2014)
Let $n = p_1^{e_1} \cdots p_t^{e_t} \geqslant 7$. *There exists a 6-valent FFC* $TL_n(a, b, 1)$ *of order* n *(with cyclic kernel)* **iff**

$$n \equiv 1 \mod 6$$

and

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

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

(a) *each solution* a *gives rise to a 6-valent FFC* $TL_n(a, \mathbf{a-1}, 1)$, *and vice versa, which is* **rotational**, **geometric** *and* $\mathbb{Z}_n.\langle[a]\rangle$*-arc-transitive with complete rotations* $[a]$ *and* $-[a^2]$;

(b) *there are exactly* 2^{t-1} *non-isomorphic such circulants.*

Optimal routing, gossiping and broadcasting

- We gave optimal routing and gossiping for $TL_n(a, a-1, 1)$ by applying the general results for first-kind Frobenius graphs and using knowledge of H-orbits on $\mathbb{Z}_n$
- Such knowledge was obtained via Eisenstein-Jacobi networks
- Formula for edge-forwarding index is messy
- Gossiping time $= (n-1)/6$
- Broadcasting time $=$ diameter $+$ (2 or 3)

HARTS (hexagonal meshes)

- A distributed real-time computing system [Chen, Shin and Kandlur, *IEEE Trans. Comp.*, 1990]
- Physically built at the Real-Time Comp. Lab, U. Michigan
- Properties studied in [Dolter, et al. *IEEE Trans. Comp.*, 1991] and [Albader, et al. *IEEE Trans. P.D.S.*, 2012]
- Denote $n_d = 3d^2 + 3d + 1$, $d \geqslant 2$
- $TL_{n_d} = TL_{n_d}(3d+2, 3d+1, 1)$ has the maximum possible order among all 6-valent geometric circulants of diameter k (Yebra, Fiol, Morillo and Alegre 1985)
- TL_{n_d} is a first-kind Frobenius graph (Thomson and Zhou 2010)
- HART: $H_d \cong TL_{n_{d-1}}$

EJ networks

C. Martinez, R. Beivide and E. Gabidulin, Perfect codes for metrics induced by circulant graphs, *IEEE Trans. I.T.*, 2007

- $\rho = (1+\sqrt{-3})/2$
- $\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$ (Eisenstein-Jacobi integers)
- $\alpha = a + b\rho \in \mathbb{Z}[\rho]$, $\alpha \neq \{0\}$
- $N(\alpha) = a^2 + ab + b^2$ (norm)
- $\mathbb{Z}[\rho]_\alpha = \mathbb{Z}[\rho]/(\alpha)$
- $H_\alpha = \{\pm[1]_\alpha, \pm[\rho]_\alpha, \pm[\rho^2]_\alpha\}$

Definition

EJ network: $EJ_\alpha = \text{Cay}(\mathbb{Z}[\rho]_\alpha, H_\alpha)$

Theorem

(Thomson and Zhou 2014)

$$\begin{aligned} & \{\textit{6-valent FFCs}\} \\ = \;\; & \{EJ_{a+b\rho} : N(a+b\rho) \equiv 1 \mod 6,\ \gcd(a,b) = 1\} \end{aligned}$$

EJ networks

C. Martinez, R. Beivide and E. Gabidulin, Perfect codes for metrics induced by circulant graphs, *IEEE Trans. I.T.*, 2007

- $\rho = (1 + \sqrt{-3})/2$
- $\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$ (Eisenstein-Jacobi integers)
- $\alpha = a + b\rho \in \mathbb{Z}[\rho]$, $\alpha \neq \{0\}$
- $N(\alpha) = a^2 + ab + b^2$ (norm)
- $\mathbb{Z}[\rho]_\alpha = \mathbb{Z}[\rho]/(\alpha)$
- $H_\alpha = \{\pm[1]_\alpha, \pm[\rho]_\alpha, \pm[\rho^2]_\alpha\}$

Definition

EJ network: $EJ_\alpha = \mathrm{Cay}(\mathbb{Z}[\rho]_\alpha, H_\alpha)$

Theorem

(Thomson and Zhou 2014)

$$\{\text{6-valent FFCs}\}$$

$$= \{EJ_{a+b\rho} : N(a + b\rho) \equiv 1 \mod 6, \ \gcd(a, b) = 1\}$$

EJ networks

C. Martinez, R. Beivide and E. Gabidulin, Perfect codes for metrics induced by circulant graphs, *IEEE Trans. I.T.*, 2007

- $\rho = (1+\sqrt{-3})/2$
- $\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$ (Eisenstein-Jacobi integers)
- $\alpha = a + b\rho \in \mathbb{Z}[\rho]$, $\alpha \neq \{0\}$
- $N(\alpha) = a^2 + ab + b^2$ (norm)
- $\mathbb{Z}[\rho]_\alpha = \mathbb{Z}[\rho]/(\alpha)$
- $H_\alpha = \{\pm[1]_\alpha, \pm[\rho]_\alpha, \pm[\rho^2]_\alpha\}$

Definition

EJ network: $EJ_\alpha = \mathrm{Cay}(\mathbb{Z}[\rho]_\alpha, H_\alpha)$

Theorem

(Thomson and Zhou 2014)

$$\{\text{6-valent FFCs}\} = \{EJ_{a+b\rho} : N(a+b\rho) \equiv 1 \mod 6,\ \gcd(a,b) = 1\}$$

EJ networks

C. Martinez, R. Beivide and E. Gabidulin, Perfect codes for metrics induced by circulant graphs, *IEEE Trans. I.T.*, 2007

- $\rho = (1 + \sqrt{-3})/2$
- $\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$ (Eisenstein-Jacobi integers)
- $\alpha = a + b\rho \in \mathbb{Z}[\rho]$, $\alpha \neq \{0\}$
- $N(\alpha) = a^2 + ab + b^2$ (norm)
- $\mathbb{Z}[\rho]_\alpha = \mathbb{Z}[\rho]/(\alpha)$
- $H_\alpha = \{\pm[1]_\alpha, \pm[\rho]_\alpha, \pm[\rho^2]_\alpha\}$

Definition

EJ network: $EJ_\alpha = \mathrm{Cay}(\mathbb{Z}[\rho]_\alpha, H_\alpha)$

Theorem

(Thomson and Zhou 2014)

$$\begin{aligned} & \{\text{6-valent FFCs}\} \\ = \ & \{EJ_{a+b\rho} : N(a+b\rho) \equiv 1 \mod 6, \ \mathtt{gcd}(a,b) = 1\} \end{aligned}$$

Rotational Cayley graphs

Let ω be a complete rotation of $\mathrm{Cay}(K, S)$.

A **fixed point** of ω is an element $g \in K \backslash \{1\}$ that is fixed by some $\omega^i \neq 1$.

Theorem

(Bermond, Kodate and Pérennes 1996)
If $\mathrm{Cay}(K, S)$ admits a complete rotation whose fixed point set is an independent set and not a vertex-cut, then

$$t(\mathrm{Cay}(K, S)) = \left\lceil \frac{|K| - 1}{|S|} \right\rceil$$

E.g. hypercubes, star graphs and multi-dimensional tori, etc.

Rotational Cayley graphs

Let ω be a complete rotation of $\mathrm{Cay}(K, S)$.

A **fixed point** of ω is an element $g \in K \backslash \{1\}$ that is fixed by some $\omega^i \neq 1$.

Theorem

(Bermond, Kodate and Pérennes 1996)
If $\mathrm{Cay}(K, S)$ admits a complete rotation whose fixed point set is an independent set and not a vertex-cut, then

$$t(\mathrm{Cay}(K, S)) = \left\lceil \frac{|K| - 1}{|S|} \right\rceil$$

E.g. hypercubes, star graphs and multi-dimensional tori, etc.

Rotational Cayley graphs

Let ω be a complete rotation of $\mathrm{Cay}(K, S)$.

A **fixed point** of ω is an element $g \in K \setminus \{1\}$ that is fixed by some $\omega^i \neq 1$.

Theorem

(Bermond, Kodate and Pérennes 1996)
If $\mathrm{Cay}(K, S)$ admits a complete rotation whose fixed point set is an independent set and not a vertex-cut, then

$$t(\mathrm{Cay}(K, S)) = \left\lceil \frac{|K| - 1}{|S|} \right\rceil$$

E.g. hypercubes, star graphs and multi-dimensional tori, etc.

Theorem

(Zhou 2009) We have

$$t(\mathrm{Cay}(K,S)) = \left\lceil \frac{|K|-1}{|S|} \right\rceil$$

if there exists $H \leqslant \mathrm{Aut}(K)$ such that H fixes S setwise and is regular on S, and $K \backslash X$ is an independent set and not a vertex-cut of Γ, where

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

In the special case where $H = \langle \omega \rangle$ for a complete rotation ω of $\mathrm{Cay}(K,S)$, we have

$$X = \{x \in K : (x^{\omega^i} = x \Rightarrow i = 0)\} \cup \{1\}$$

and so $K \backslash X$ is the set of fixed points of ω. The result above generalises the previous result of BKP.

Theorem

(Zhou 2009) We have

$$t(\mathrm{Cay}(K,S)) = \left\lceil \frac{|K|-1}{|S|} \right\rceil$$

if there exists $H \leqslant \mathrm{Aut}(K)$ such that H fixes S setwise and is regular on S, and $K \backslash X$ is an independent set and not a vertex-cut of Γ, where

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

In the special case where $H = \langle \omega \rangle$ for a complete rotation ω of $\mathrm{Cay}(K,S)$, we have

$$X = \{x \in K : (x^{\omega^i} = x \Rightarrow i = 0)\} \cup \{1\}$$

and so $K \backslash X$ is the set of fixed points of ω. The result above generalises the previous result of BKP.

Classification of rotational FFCs

Theorem

(Thomson and Zhou 2014)
Let $n = p_1^{e_1} \ldots p_t^{e_t}$ *and* $D = \mathtt{gcd}(p_1 - 1, \ldots, p_t - 1)$.

(a) $\exists$ *a rotational FFC with kernel* $\mathbb{Z}_n$ *and valency* d **iff** n *is odd and* d *is an even divisor of* D.

(b) $\varphi(d)^{l-1}$ *such circulants (pairwise non-isomorphic)*

(c) *Each is isomorphic to* $\mathrm{Cay}(\mathbb{Z}_n, \langle [h] \rangle)$, *where* $h = \sum_{i=1}^{t} (n/p_i^{e_i}) b_i h_i$, *with* $b_i (n/p_i^{e_i}) \equiv 1 \pmod{p_i^{e_i}}$ *and* $h_i \equiv \eta_i^{m_i \varphi(p_i^{e_i})/d} \pmod{p_i^{e_i}}$ *for a fixed primitive root* η_i *mod* $p_i^{e_i}$ *and an integer* m_i *coprime to* d.

Special case: if $n = p^e$, then for every even divisor d of $p - 1$, there is a unique rotational FFC of order p^e and valency d.

An example

Example

Let $n = 6253 = 13^2 \times 37$, so that $p_1 = 13$, $p_2 = 37$, and $D = \texttt{gcd}(12, 36) = 12$.

Choose $\eta_1 = \eta_2 = 2$, which is a primitive root mod 13 as well as a primitive root mod 37.

We have $b_1 \equiv 37^{-1} \equiv 32 \pmod{13^2}$ and $b_2 \equiv (13^2)^{-1} \equiv 30 \pmod{37}$.

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

An example

Example

Let $n = 6253 = 13^2 \times 37$, so that $p_1 = 13$, $p_2 = 37$, and $D = \mathrm{gcd}(12, 36) = 12$.

Choose $\eta_1 = \eta_2 = 2$, which is a primitive root mod 13 as well as a primitive root mod 37.

We have $b_1 \equiv 37^{-1} \equiv 32 \pmod{13^2}$ and $b_2 \equiv (13^2)^{-1} \equiv 30 \pmod{37}$.

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

An example

Example

Let $n = 6253 = 13^2 \times 37$, so that $p_1 = 13$, $p_2 = 37$, and $D = \mathtt{gcd}(12, 36) = 12$.

Choose $\eta_1 = \eta_2 = 2$, which is a primitive root mod 13 as well as a primitive root mod 37.

We have $b_1 \equiv 37^{-1} \equiv 32 \pmod{13^2}$ and $b_2 \equiv (13^2)^{-1} \equiv 30 \pmod{37}$.

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

An example

Example

Let $n = 6253 = 13^2 \times 37$, so that $p_1 = 13$, $p_2 = 37$, and $D = \gcd(12, 36) = 12$.

Choose $\eta_1 = \eta_2 = 2$, which is a primitive root mod 13 as well as a primitive root mod 37.

We have $b_1 \equiv 37^{-1} \equiv 32 \pmod{13^2}$ and $b_2 \equiv (13^2)^{-1} \equiv 30 \pmod{37}$.

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

d	(m_1, m_2)	(h_1, h_2)	h
2			$-[1]$
4	(1, 1)	(99, 31)	$-[746]$
4	(1, 3)	(99, 6)	$-[2436]$
6	(1, 1)	(147, 27)	$-[1712]$
6	(5, 5)	(147, 11)	$-[1543]$
12	(1, 1)	(80, 8)	$-[2286]$
12	(1, 5)	(80, 23)	$-[1272]$
12	(1, 7)	(80, 29)	$-[2117]$
12	(1, 11)	(80, 14)	$+[3122]$

Table: All rotational first-kind Frobenius circulants with kernel $\mathbb{Z}_{6253}$

Rotational FFCs

Theorem
(Thomson and Zhou 2014)
We know exactly when a FFC can be embedded on a closed orientable surface as a balanced regular Cayley map.

Theorem
(Conder and Tucker 2012+)
Regular Cayley maps for the cyclic group of every possible order are classified.

$2p$-valent FFCs

Theorem

(Zhou 2014)
Let p be an odd prime and $n \geqslant 2p+1$.
A $2p$-valent circulant $C(n,S)$ with $[1] \in S$ is a FFC with cyclic kernel if and only if

$$n \equiv 1 \mod 2p$$

and

$$S = \langle [a] \rangle$$

for some a such that $a^p + 1 \equiv 0 \mod n$ and
$a^i \pm 1, 1 \leqslant i \leqslant p-1$ are all coprime to n.

In this case $C(n, \langle [a] \rangle)$ is a $\mathbb{Z}_n.\langle [a] \rangle$-arc transitive first-kind $\mathbb{Z}_n.\langle [a] \rangle$-Frobenius circulant.

$2p^2$-valent FFCs

Theorem

(Zhou 2014)
All $2p^2$-valent FFCs are classified, for all primes p.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Cyclotomic graphs

- ζ_m: primitive mth root of unity, e.g. $\zeta_m = e^{2\pi i/m}$, $m \geqslant 2$
- $\mathbb{Q}(\zeta_m)$: corresponding cyclotomic field
- $\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_i \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$

Definition

Le $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Denote

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leqslant i \leqslant m-1\}.$$

Call

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

the mth **cyclotomic graph** w.r.t. A.

In other words, $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent in $G_m(A)$ iff $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i.

Two special cases

Example

Consider $m = 2$ and $\zeta_2 = i$.

$\mathbb{Z}[i]$ is an Euclidean domain and so all ideals are principal ideals (α).

$G_2((\alpha))$ is called a **Gaussian network**.

Example

Consider $m = 3$ and $\zeta_3 = \rho = (1 + \sqrt{3}i)/2$.

$\mathbb{Z}[\rho]$ is also Euclidean.

$G_3((\alpha)) = EJ_\alpha$ is an EJ network.

There are precisely 29 cyclotomic fields $\mathbb{Q}(\zeta_m)$ such that $\mathbb{Z}[\zeta_m]$ is a principal ideal domain.

Two special cases

Example

Consider $m = 2$ and $\zeta_2 = i$.

$\mathbb{Z}[i]$ is an Euclidean domain and so all ideals are principal ideals (α).

$G_2((\alpha))$ is called a **Gaussian network**.

Example

Consider $m = 3$ and $\zeta_3 = \rho = (1 + \sqrt{3}i)/2$.

$\mathbb{Z}[\rho]$ is also Euclidean.

$G_3((\alpha)) = EJ_\alpha$ is an EJ network.

There are precisely 29 cyclotomic fields $\mathbb{Q}(\zeta_m)$ such that $\mathbb{Z}[\zeta_m]$ is a principal ideal domain.

Two special cases

Example

Consider $m = 2$ and $\zeta_2 = i$.

$\mathbb{Z}[i]$ is an Euclidean domain and so all ideals are principal ideals (α).

$G_2((\alpha))$ is called a **Gaussian network**.

Example

Consider $m = 3$ and $\zeta_3 = \rho = (1 + \sqrt{3}i)/2$.

$\mathbb{Z}[\rho]$ is also Euclidean.

$G_3((\alpha)) = EJ_\alpha$ is an EJ network.

There are precisely 29 cyclotomic fields $\mathbb{Q}(\zeta_m)$ such that $\mathbb{Z}[\zeta_m]$ is a principal ideal domain.

Norm

- $N(A)$: **norm** of A, i.e. the size of $\mathbb{Z}[\zeta_m]/A$ (finite by number theory)
- $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$: **norm** of $\alpha \in \mathbb{Q}(\zeta_m)$
- $N(\alpha) \geqslant 0$ is an integer for $\alpha \in \mathbb{Z}[\zeta_m]$
- $N(\alpha) = N((\alpha))$ for $\alpha \in \mathbb{Z}[\zeta_m]$

Norm

- $N(A)$: **norm** of A, i.e. the size of $\mathbb{Z}[\zeta_m]/A$ (finite by number theory)
- $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$: **norm** of $\alpha \in \mathbb{Q}(\zeta_m)$
- $N(\alpha) \geqslant 0$ is an integer for $\alpha \in \mathbb{Z}[\zeta_m]$
- $N(\alpha) = N((\alpha))$ for $\alpha \in \mathbb{Z}[\zeta_m]$

Norm

- $N(A)$: **norm** of A, i.e. the size of $\mathbb{Z}[\zeta_m]/A$ (finite by number theory)
- $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$: **norm** of $\alpha \in \mathbb{Q}(\zeta_m)$
- $N(\alpha) \geqslant 0$ is an integer for $\alpha \in \mathbb{Z}[\zeta_m]$
- $N(\alpha) = N((\alpha))$ for $\alpha \in \mathbb{Z}[\zeta_m]$

Norm

- $N(A)$: **norm** of A, i.e. the size of $\mathbb{Z}[\zeta_m]/A$ (finite by number theory)
- $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$: **norm** of $\alpha \in \mathbb{Q}(\zeta_m)$
- $N(\alpha) \geqslant 0$ is an integer for $\alpha \in \mathbb{Z}[\zeta_m]$
- $N(\alpha) = N((\alpha))$ for $\alpha \in \mathbb{Z}[\zeta_m]$

Cyclotomic graphs

Theorem

(Zhou 2014)

(a) *$G_m(A)$ is finite, connected, undirected with order $N(A)$ and valency $|E_m/A| \leqslant 2m$;*

(b) *$G_m(A)$ has valency $2m$ iff $1 \pm \zeta_m^i \notin A$ for $1 \leqslant i \leqslant m-1$; in particular, if $N(\alpha) \geqslant 3$ for every $\alpha \in A$, then $G_m(A)$ has valency $2m$;*

Cyclotomic graphs

Theorem

(Zhou 2014)

(a) $G_m(A)$ *is finite, connected, undirected with order* $N(A)$ *and valency* $|E_m/A| \leqslant 2m$;

(b) $G_m(A)$ *has valency* $2m$ *iff* $1 \pm \zeta_m^i \notin A$ *for* $1 \leqslant i \leqslant m-1$; *in particular, if* $N(\alpha) \geqslant 3$ *for every* $\alpha \in A$, *then* $G_m(A)$ *has valency* $2m$;

Theorem

(cont'd)

(c) *if $G_m(A)$ has valency $2m$, letting*

$$H_A := \{(-\zeta_m)^i + A : 0 \leqslant i \leqslant 2m-1\},$$

then $(\mathbb{Z}[\zeta_m]/A).H_A$ is isomorphic to a subgroup of $\mathrm{Aut}(G_m(A))$ *and is transitive on the vertex set of $G_m(A)$; moreover, if m is odd, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is arc-transitive on $G_m(A)$, and if m is even, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is edge-transitive but not arc-transitive on $G_m(A)$;*

(d) *if $G_m(A)$ has valency $2m$, then it is rotational.*

Cyclotomic graphs

Theorem

(cont'd)

(c) *if $G_m(A)$ has valency $2m$, letting*

$$H_A := \{(-\zeta_m)^i + A : 0 \leqslant i \leqslant 2m-1\},$$

then $(\mathbb{Z}[\zeta_m]/A).H_A$ is isomorphic to a subgroup of $\mathrm{Aut}(G_m(A))$ and is transitive on the vertex set of $G_m(A)$; moreover, if m is odd, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is arc-transitive on $G_m(A)$, and if m is even, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is edge-transitive but not arc-transitive on $G_m(A)$;

(d) *if $G_m(A)$ has valency $2m$, then it is rotational.*

Cyclotomic graphs

Theorem

(cont'd)

(c) *if $G_m(A)$ has valency $2m$, letting*

$$H_A := \{(-\zeta_m)^i + A : 0 \leqslant i \leqslant 2m-1\},$$

then $(\mathbb{Z}[\zeta_m]/A).H_A$ is isomorphic to a subgroup of $\mathrm{Aut}(G_m(A))$ and is transitive on the vertex set of $G_m(A)$; moreover, if m is odd, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is arc-transitive on $G_m(A)$, and if m is even, then $(\mathbb{Z}[\zeta_m]/A).H_A$ is edge-transitive but not arc-transitive on $G_m(A)$;

(d) *if $G_m(A)$ has valency $2m$, then it is rotational.*

Circulant cyclotomic graphs

Theorem

(Zhou 2014)
Let $m \geqslant 3$ and $n \geqslant 5$ be odd positive integers, and let a be an integer with $1 < a < n$.
Suppose that $n \equiv 1 \mod 2m$, $a^m + 1 \equiv 0 \mod n$, and $a^i \pm 1$ for $1 \leqslant i \leqslant m - 1$ are all coprime to n.
Then $C(n, \langle [a] \rangle)$ is isomorphic to an mth cyclotomic graph of valency $2m$.

When is the converse true? (under investigation)

Choosing $m = p$, we obtain:

Corollary

All $2p$-valent FFCs are cyclotomic.

Circulant cyclotomic graphs

Theorem

(Zhou 2014)
Let $m \geqslant 3$ and $n \geqslant 5$ be odd positive integers, and let a be an integer with $1 < a < n$.
Suppose that $n \equiv 1 \mod 2m$, $a^m + 1 \equiv 0 \mod n$, and $a^i \pm 1$ for $1 \leqslant i \leqslant m-1$ are all coprime to n.
Then $C(n, \langle [a] \rangle)$ is isomorphic to an mth cyclotomic graph of valency $2m$.

When is the converse true? (under investigation)

Choosing $m = p$, we obtain:

Corollary

All 2p-valent FFCs are cyclotomic.

Circulant cyclotomic graphs

Theorem

(Zhou 2014)
Let $m \geqslant 3$ and $n \geqslant 5$ be odd positive integers, and let a be an integer with $1 < a < n$.
Suppose that $n \equiv 1 \mod 2m$, $a^m + 1 \equiv 0 \mod n$, and $a^i \pm 1$ for $1 \leqslant i \leqslant m-1$ are all coprime to n.
Then $C(n, \langle [a] \rangle)$ is isomorphic to an mth cyclotomic graph of valency $2m$.

When is the converse true? (under investigation)

Choosing $m = p$, we obtain:

Corollary

All $2p$-valent FFCs are cyclotomic.

Distance in cyclotomic graphs

Let $\alpha = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$. Define the **Manhattan weight** by

$$|\alpha| := \sum_{i=0}^{m-1} |a_i|.$$

For $\bar{\alpha} = \alpha + A$, define the **Mannheim weight** by

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\}$$

Lemma

(Zhou 2014)

(a) *$\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m(A)$ iff $\|\bar{\alpha} - \bar{\beta}\| = 1$;*

(b) *In general, the distance in $G_m(A)$ between $\bar{\alpha}$ and $\bar{\beta}$ is equal to $\|\bar{\alpha} - \bar{\beta}\|$.*

Distance in cyclotomic graphs

Let $\alpha = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$. Define the **Manhattan weight** by

$$|\alpha| := \sum_{i=0}^{m-1} |a_i|.$$

For $\bar{\alpha} = \alpha + A$, define the **Mannheim weight** by

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\}$$

Lemma

(Zhou 2014)

(a) *$\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m(A)$ iff $\|\bar{\alpha} - \bar{\beta}\| = 1$;*

(b) *In general, the distance in $G_m(A)$ between $\bar{\alpha}$ and $\bar{\beta}$ is equal to $\|\bar{\alpha} - \bar{\beta}\|$.*

Distance in cyclotomic graphs

Let $\alpha = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$. Define the **Manhattan weight** by

$$|\alpha| := \sum_{i=0}^{m-1} |a_i|.$$

For $\bar{\alpha} = \alpha + A$, define the **Mannheim weight** by

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\}$$

Lemma

(Zhou 2014)

(a) *$\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m(A)$ iff $\|\bar{\alpha} - \bar{\beta}\| = 1$;*

(b) *In general, the distance in $G_m(A)$ between $\bar{\alpha}$ and $\bar{\beta}$ is equal to $\|\bar{\alpha} - \bar{\beta}\|$.*

Distance in cyclotomic graphs

Let $\alpha = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$. Define the **Manhattan weight** by

$$|\alpha| := \sum_{i=0}^{m-1} |a_i|.$$

For $\bar{\alpha} = \alpha + A$, define the **Mannheim weight** by

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\}$$

Lemma

(Zhou 2014)

(a) *$\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m(A)$ iff $\|\bar{\alpha} - \bar{\beta}\| = 1$;*

(b) *In general, the distance in $G_m(A)$ between $\bar{\alpha}$ and $\bar{\beta}$ is equal to $\|\bar{\alpha} - \bar{\beta}\|$.*

Other results on cyclotomic graphs

- Hamilton decomposability of $G_m((\alpha))$ when $N(\alpha)$ is a prime
- Necessary and sufficient condition for D/A to be a perfect t-dominating set (equivalently a perfect t-error correcting group code of length one), where D is an ideal of $\mathbb{Z}[\zeta_m]$ with $A \subseteq D$
- In particular, improvements of some known results on perfect t-dominating sets in Gaussian and EJ networs
- Quotients of cyclotomic graphs and covers

thank you