Cubic graphical regular representations of non-abelian simple groups

Shasha ZHENG
University of Melbourne

Based on joint work with Binzhou XIA and Sanming ZHOU

Group Theory Seminars, SUSTech, May 2022

Outline

1. Cayley (di)graphs and GRRs (DRRs)
2. Cubic GRRs of finite non-abelian simple groups
   - Cubic GRRs of some classical simple groups

Digraph

A digraph Γ is an ordered pair $(V(\Gamma), A(\Gamma))$, where $V(\Gamma)$ is the set of vertices and $A(\Gamma)$ is the set of ordered pairs of vertices called arcs.

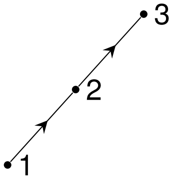


Figure: Digraph Γ_1

- $V(\Gamma_1) = \{1, 2, 3\}$.
- $A(\Gamma_1) = \{(1, 2), (2, 3)\}$.

Digraph

For a digraph Γ, if $A(\Gamma)$ is symmetric, then Γ is called an undirected graph (or a graph for short).

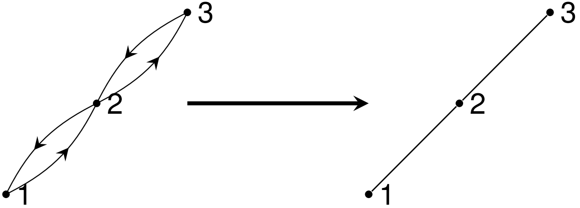


Figure: Graph Γ_2

$$A(\Gamma_2) = \{(1,2),(2,1),(2,3),(3,2)\} \longrightarrow E(\Gamma_2) = \{\{1,2\},\{2,3\}\}.$$

Digraph automorphism

For $\Gamma = (V(\Gamma), A(\Gamma))$ and $\sigma \in \mathrm{Sym}(V(\Gamma))$, if σ preserves the adjacency of Γ, then σ is called an automorphism of Γ.

Figure: Digraph Γ_1

Figure: Graph Γ_2

- 1 is the unique automorphism of Γ_1, but Γ_2 has $(1, 3)$ as another automorphism.

Digraph automorphism

For $\Gamma = (V(\Gamma), A(\Gamma))$ and $\sigma \in \mathrm{Sym}(V(\Gamma))$, if σ preserves the adjacency of Γ, then σ is called an automorphism of Γ.

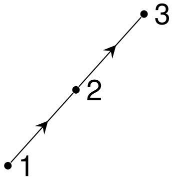


Figure: Digraph Γ_1

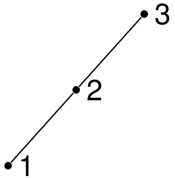


Figure: Graph Γ_2

- 1 is the unique automorphism of Γ_1, but Γ_2 has $(1, 3)$ as another automorphism.

Digraph symmetries

Definition 1

All automorphisms of Γ form a group $\mathrm{Aut}(\Gamma)$, called the full automorphism group of Γ.

Definition 2

If $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$, $A(\Gamma)$ or $E(\Gamma)$, then Γ is called vertex-transitive, arc-transitive or edge-transitive respectively.

- A digraph is called symmetric if it is both vertex-transitive and arc-transitive.

Digraph symmetries

Definition 1

All automorphisms of Γ form a group $\mathrm{Aut}(\Gamma)$, called the full automorphism group of Γ.

Definition 2

If $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$, $A(\Gamma)$ or $E(\Gamma)$, then Γ is called vertex-transitive, arc-transitive or edge-transitive respectively.

- A digraph is called symmetric if it is both vertex-transitive and arc-transitive.

Digraph symmetries

Definition 1

All automorphisms of Γ form a group $\mathrm{Aut}(\Gamma)$, called the full automorphism group of Γ.

Definition 2

If $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$, $A(\Gamma)$ or $E(\Gamma)$, then Γ is called vertex-transitive, arc-transitive or edge-transitive respectively.

- A digraph is called symmetric if it is both vertex-transitive and arc-transitive.

Cayley digraph

Definition 3

Let G be a group and $1 \notin S \subset G$. The Cayley digraph of G with respect to S, denoted by $\mathrm{Cay}(G, S)$, is defined as the digraph with vertex set G and arc set $\{(u, v) : vu^{-1} \in S, u, v \in G\}$.

- A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if Γ admits a regular group of automorphisms isomorphic to G.

Cayley digraph

Definition 3

Let G be a group and $1 \notin S \subset G$. The Cayley digraph of G with respect to S, denoted by $\mathrm{Cay}(G, S)$, is defined as the digraph with vertex set G and arc set $\{(u, v) : vu^{-1} \in S, u, v \in G\}$.

- A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if Γ admits a regular group of automorphisms isomorphic to G.

Cayley digraph

Example

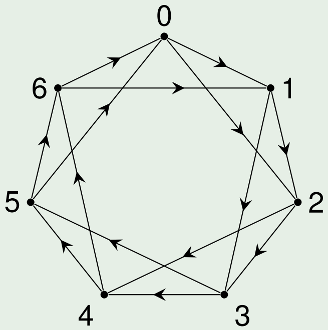


Figure: Cayley digraph $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2\})$

Cayley digraph

Example

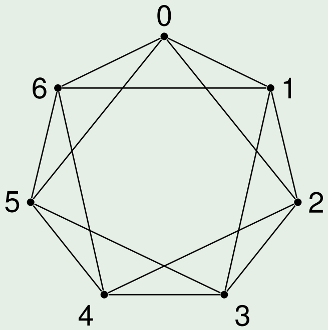


Figure: Cayley graph $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2, 5, 6\})$

Right regular representation

For a given group G, every element $g \in G$ induces a right translation $\mathrm{R}(g)$ on G as follows.

$$\begin{aligned} \mathrm{R}(g): \quad G &\to G \\ u &\mapsto ug \end{aligned}$$

Let

$$\mathrm{R}(G) = \{\mathrm{R}(g) \mid g \in G\}.$$

It is called the right regular representation of G.

- $\mathrm{R}(G) \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ and it is transitive on G.
- All Cayley digraphs are vertex-transitive.

Right regular representation

For a given group G, every element $g \in G$ induces a right translation $\mathrm{R}(g)$ on G as follows.

$$\begin{aligned} \mathrm{R}(g): \quad G &\to G \\ u &\mapsto ug \end{aligned}$$

Let

$$\mathrm{R}(G) = \{\mathrm{R}(g) \mid g \in G\}.$$

It is called the right regular representation of G.

- $\mathrm{R}(G) \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ and it is transitive on G.
- All Cayley digraphs are vertex-transitive.

Normal Cayley digraph

Definition 4

A Cayley digraph $\mathrm{Cay}(G, S)$ is said to be normal for G if

$$\mathrm{R}(G) \trianglelefteq \mathrm{Aut}(\mathrm{Cay}(G, S)).$$

- If a Cayley digraph is normal, then it is much easier to determine its full automorphism group.
- $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2\})$ and $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2, 5, 6\})$ are normal.
  —All Cayley digraphs of $\mathbb{Z}_p$ (p a prime), other than K_p or pK_1, are normal.

M. Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, Discrete Math. 182 (1998) 309–319.

DRR and GRR

Definition 5

For a Cayley (di)graph $\mathrm{Cay}(G, S)$, if $R(G) = \mathrm{Aut}(\mathrm{Cay}(G, S))$, then $\mathrm{Cay}(G, S)$ is called a (di)graphical regular representation (GRR or DRR for short) of G.

- All DRRs (GRRs) are normal.
- A GRR (DRR) of G is a Cayley (di)graph of G with smallest possible full automorphism group when G admits one.
- Q (König, 1936): given a group G, is there a (di)graph whose automorphism group is isomorphic to G?

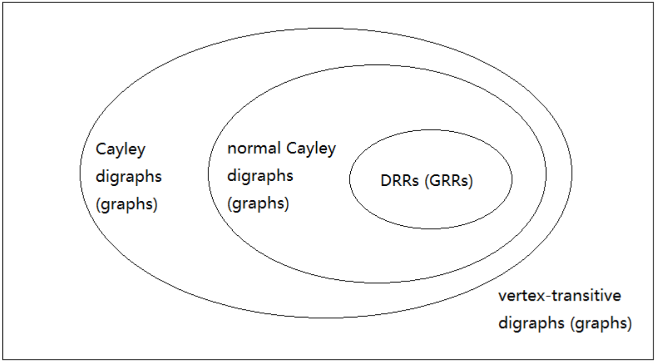
DRR and GRR

Definition 5

For a Cayley (di)graph $\mathrm{Cay}(G, S)$, if $R(G) = \mathrm{Aut}(\mathrm{Cay}(G, S))$, then $\mathrm{Cay}(G, S)$ is called a (di)graphical regular representation (GRR or DRR for short) of G.

- All DRRs (GRRs) are normal.
- A GRR (DRR) of G is a Cayley (di)graph of G with smallest possible full automorphism group when G admits one.
- Q (König, 1936): given a group G, is there a (di)graph whose automorphism group is isomorphic to G?

Relationships



Some subclasses of vertex-transitive digraphs

Graphical regular representation

Theorem (Godsil 1978)

Apart from abelian groups of exponent at least three, generalized dicyclic groups and the following thirteen other groups:

(1) $\mathrm{C}_2^2, \mathrm{C}_2^3, \mathrm{C}_2^4, D_6, D_8, D_{10}, A_4, \mathrm{Q}_8 \times \mathrm{C}_3, \mathrm{Q}_8 \times \mathrm{C}_4$,

(2) $\langle a, b \mid a^8 = b^2 = 1, b^{-1}ab = a^5 \rangle$,

(3) $\langle a, b, c \mid a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle$,

(4) $\langle a, b, c \mid a^3 = b^3 = c^2 = (ac)^2 = (bc)^2 = 1, ab = ba \rangle$ and

(5) $\langle a, b, c \mid a^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \rangle$,

every finite group admits a GRR.

Fang, Li, Wang and Xu's conjecture

There is special interest in GRRs of a prescribed valency.

Conjecture 1 (Fang, Li, Wang and Xu, 2002)

Every finite non-abelian simple group admits a cubic GRR.

- Xia and Fang found that this conjecture fails for $\mathrm{PSL}_2(7)$.

X.G. Fang, C.H. Li, J. Wang and M.Y. Xu, On cubic Cayley graphs of finite simple groups, Discrete Math. 244 (2002) 67–75.

B. Xia and T. Fang, Cubic graphical regular representations of $\mathrm{PSL}_2(q)$, Discrete Math. 339 (8) (2016) 2051–2055.

Fang and Xia's conjecture

Conjecture 2 (Fang and Xia, 2016)

Except a finite number of cases, every finite non-abelian simple group has a cubic GRR.

- An alternating group? (Godsil, 1983.)
- A classical group?
- An exceptional group of Lie type?
  - $\mathrm{Sz}(q)$ with $q = 2^{2n+1} \geq 8$. (Fang et al., 2002.)
  - $\mathrm{Ree}(q)$ with $q = 3^{2n+1} \geq 27$. (2022+.)
- A sporadic simple group?

B. Xia and T. Fang, Cubic graphical regular representations of $\mathrm{PSL}_2(q)$, Discrete Math. 339 (8) (2016) 2051–2055.

Cubic GRRs of finite non-abelian simple groups

- If $\mathrm{Cay}(G, S)$ is a GRR of G, then we necessarily have $\langle S\rangle = G$ and $\mathrm{Aut}(G, S) = 1$, where

$$\mathrm{Aut}(G, S) = \{\alpha \in \mathrm{Aut}(G) : S^{\alpha} = S\}.$$

- A list of finite non-abelian simple groups G for which a cubic Cayley graph $\mathrm{Cay}(G, S)$ is a GRR if and only if $\langle S\rangle = G$ and $\mathrm{Aut}(G, S) = 1$ was given.
    - It contains all sporadic simple groups and all simple groups of exceptional Lie type.

B. Xia, Cubic graphical regular representations of $\mathrm{PSL}_3(q)$, Discrete Math. 343 (1) (2020) 111646.

Cubic GRRs of finite non-abelian simple groups

The list:

(i) G is a sporadic simple group;

(ii) $G = A_n$ with $n \notin \{47\} \cup \{2^m - 1 \mid m \geq 4\}$;

(iii) G is a simple group of exceptional Lie type;

(iv) G is a classical simple group of odd characteristic;

(v) $G = \mathrm{PSL}_n(q)$ with q even and $n \geq 4$ such that either n is odd and $q > 2$ or $\gcd(n, q - 1) > 1$;

(vi) $G = \mathrm{PSU}_n(q)$ with q even and $n \geq 6$ such that either n is odd or $\gcd(n, q + 1) > 1$;

(vii) $G = \mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$, $\mathrm{PSU}_3(q)$, $\mathrm{PSU}_4(q)$, $\mathrm{PSU}_5(q)$ or $\mathrm{PSp}_4(q)$, where q is even.

B. Xia, Cubic graphical regular representations of $\mathrm{PSL}_3(q)$, Discrete Math. 343 (1) (2020) 111646.

Cubic GRRs of finite non-abelian simple groups

- For every finite non-abelian simple group G except A_7, $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$, there exists a pair of generators (x, y) of G where y is an involution such that $\mathrm{Aut}(G, \{x, x^{-1}, y\}) = 1$.
  - In particular, all sporadic simple groups and simple groups of exceptional Lie type admit cubic GRRs.

D. Leemans and M.W. Liebeck, Chiral polyhedra and finite simple groups, Bull. London Math. Soc. 49 (2017) 581–592.

Conjecture 2 for classical simple groups

- Most families of classical groups are known to admit cubic GRRs.

B. Xia, On cubic graphical regular representations of finite simple groups, J. Combin. Theory Ser. B 141 (2020) 1–30.

B. Xia and T. Fang, Cubic graphical regular representations of $\mathrm{PSL}_2(q)$, Discrete Math. 339 (8) (2016) 2051–2055.

B. Xia, Cubic graphical regular representations of $\mathrm{PSL}_3(q)$, Discrete Math. 343 (1) (2020) 111646.

Conjecture 2 for classical simple groups

To settle Conjecture 2, the remaining families of groups that need to be considered are:

- $\mathrm{PSU}_3(q)$ with $q \neq 2$,
- $\mathrm{PSL}_4(q)$, $\mathrm{PSL}_6(q)$ (where $\gcd(6, q-1) = 1$), $\mathrm{PSL}_8(q)$, $\mathrm{PSp}_6(q)$, $\mathrm{PSp}_8(q)$, $\mathrm{P\Omega}_8^{\pm}(q)$, $\mathrm{P\Omega}_{10}^{\pm}(q)$, and $\mathrm{P\Omega}_{12}^{\pm}(q)$ with q even.
    - If a group G has no proper subgroup of index at most 47, then for an involution y and an element x of an odd prime order in G, $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ is a GRR of G if and only if $G = \langle x, y \rangle$ and $\mathrm{Aut}(G, \{x, x^{-1}, y\}) = 1$.

Primitive prime divisor

For a pair of positive integers (a, m) with $a \geq 2$ and $m \geq 2$, we call a prime divisor r of $a^m - 1$ a primitive prime divisor of (a, m) if r does not divide $a^i - 1$ for every positive integer $i < m$.

Denote the set of primitive prime divisors of (a, m) by $\mathrm{ppd}(a, m)$.

- By Zsigmondy's theorem, if $(a, m) \neq (2^k - 1, 2), (2, 6)$, then $\mathrm{ppd}(a, m)$ is not empty.

Our main result

Theorem 1 (Xia, Z and Zhou, 2022+)

Let G be a finite simple group and $r \in \mathrm{ppd}(2, ef)$, where G and e are given in the table with $q = 2^f$, $f \geq 1$, and let x be any fixed element of G with order r. Then for a random involution y of G, the probability of $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ being a GRR of G approaches 1 as q approaches infinity.

G	Conditions	e
$\mathrm{PSL}_n(q)$	$n = 4, 6$ or 8, q even	n
$\mathrm{PSp}_n(q)$	$n = 6$ or 8, q even	n
$\mathrm{P\Omega}_n^+(q)$	$n = 8, 10$ or 12, q even	$n - 2$
$\mathrm{P\Omega}_n^-(q)$	$n = 8, 10$ or 12, q even	n

Table: The pairs (G, e) in Theorem 3

Methodologies

For a subset A of a group G, denote by $I_2(A)$ the set of involutions of G in A, and set $i_2(A) = |I_2(A)|$.

Let G, q and x be as in Theorem 3. Define

$$K(x) = \{y \in I_2(G) : G = \langle x, y \rangle\},$$

$$L(x) = \{y \in I_2(G) : \mathrm{Aut}(G, \{x, x^{-1}, y\}) = 1\},$$

$$\mathrm{Inv}(x) = \{\alpha \in I_2(\mathrm{Aut}(G)) : x^{\alpha} = x^{-1}\},$$

$\mathcal{M}(x)$: the set of maximal subgroups of G containing x.

Methodologies

If $q \geq 4$ for $G = \mathrm{PSL}_4(q)$ and $q \geq 2$ for any other G, then for a random involution y of G, the probability $P(x)$ of $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ being a GRR of G is given by

$$P(x) = \frac{|K(x) \cap L(x)|}{i_2(G)}.$$

Moreover,

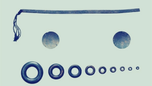
$$P(x) \geq 1 - \frac{i_2\left(\cup_{M \in \mathcal{M}(x)} M\right)}{i_2(G)} - \frac{\sum_{\alpha \in \mathrm{Inv}(x)} i_2(\mathbf{C}_G(\alpha))}{i_2(G)}.$$

Example: $\mathrm{PSL}_4(q)$

$G = \mathrm{PSL}_4(q)$ with $q \geq 4$ even

$$P(x) \geq 1 - \frac{i_2\left(\cup_{M \in \mathcal{M}(x)} M\right)}{i_2(G)} - \frac{\sum_{\alpha \in \mathrm{Inv}(x)} i_2(\mathbf{C}_G(\alpha))}{i_2(G)} > 1 - 5q^{-1}.$$

- $i_2(G) > q^5(q^3 - 1)$.
- $i_2\left(\cup_{M \in \mathcal{M}(x)} M\right) < 3q^7/2$.
- $i_2(\mathbf{C}_G(\alpha)) < 2q^4$ for $\alpha \in \mathrm{Inv}(x)$.
- $|\mathrm{Inv}(x)| \leq 13q^3/8$.



Spiga's conjectures

Conjecture 3 (Spiga, 2018)

For finite non-abelian simple groups, the proportion of cubic Cayley graphs of a given group that are GRRs approaches 1 as the order of the group approaches infinity.

- Theorem 1 provides evidence in some sense to support this conjecture for those families of groups.

P. Spiga, Cubic graphical regular representations of finite non-abelian simple groups, Commun. Algebra 46 (6) (2018) 2440–2450.

Spiga's conjectures

Conjecture 4 (Spiga, 2018)

Except $\mathrm{PSL}_2(q)$ and a finite number of other cases, every finite non-abelian simple group G contains an element x and an involution y such that $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ is a GRR of G.

- Both $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ form infinite families of counterexamples.

P. Spiga, Cubic graphical regular representations of finite non-abelian simple groups, Commun. Algebra 46 (6) (2018) 2440–2450.

A. Breda d'Azevedo and D.A. Catalano, Strong map-symmetry of $\mathrm{SL}(3, K)$ and $\mathrm{PSL}(3, K)$ for every finite field K, J. Algebra Appl. 20 (04) (2021) p.2150048.

A modified version of Conjecture 4

Our work together with several known results implies that we can save Conjecture 4 by adding $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ to the list of exceptional groups.

Theorem 2 (Xia, Z and Zhou, 2022+)

Except $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$, $\mathrm{PSU}_3(q)$ and a finite number of other cases, every finite non-abelian simple group G contains an element x and an involution y such that $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ is a GRR of G.

Fang and Xia's conjecture

Conjecture 2 (Fang and Xia, 2016)

Except for a finite number of cases, every finite non-abelian simple group has a cubic GRR.

- Note that $\mathrm{PSL}_2(q)$ with $q \notin \{2, 3, 7\}$ and $\mathrm{PSL}_3(q)$ with $q \neq 2$ admit cubic GRRs with connection sets consisting of three involutions.
- How about $\mathrm{PSU}_3(q)$?
  For a prime power q, the group $\mathrm{PSU}_3(q)$ has a cubic GRR if and only if $q \geq 4$.

J.J. Li, B. Xia, X.Q. Zhang and Z, Cubic graphical regular representations of $\mathrm{PSU}_3(q)$, arXiv preprint (2022) arXiv: 2201.04307.

Fang and Xia's conjecture

Theorem 3 (Xia, Z and Zhou, 2022+)

Except for a finite number of cases, every finite non-abelian simple group has a cubic GRR.

Thank you !