Discrete Mathematics 339 (2016) 2051–2055

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

Cubic graphical regular representations of $\mathrm{PSL}_2(q)$

Binzhou Xia *, Teng Fang

Beijing International Center for Mathematical Research, Peking University, Beijing, 100871, PR China

ARTICLE INFO

Article history:
Received 28 July 2015
Received in revised form 1 March 2016
Accepted 9 March 2016
Available online 26 April 2016

Keywords:
Cayley graph
Cubic graph
Graphical regular representation
Projective special linear group

ABSTRACT

We study cubic graphical regular representations of the finite simple groups $\mathrm{PSL}_2(q)$. It is shown that such graphical regular representations exist if and only if $q \neq 7$, and the generating set must consist of three involutions.

1. Introduction

Given a group G and a subset $S \subset G$ such that $1 \notin S$ and $S = S^{-1} := \{g^{-1} \mid g \in S\}$, the *Cayley graph* $\mathrm{Cay}(G, S)$ of G is the graph with vertex set G such that two vertices x, y are adjacent if and only if $yx^{-1} \in S$. It is easy to see that $\mathrm{Cay}(G, S)$ is connected if and only if S generates the group G. If one identifies G with its right regular representation, then G is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$. We call $\mathrm{Cay}(G, S)$ a *graphical regular representation* (*GRR* for short) of G if $\mathrm{Aut}(\mathrm{Cay}(G, S)) = G$. The problem of seeking graphical regular representations for given groups has been investigated for a long time. A major accomplishment for this problem is the determination of finite groups without a GRR, see [1, 16g]. It turns out that most finite groups admit at least one GRR. For instance, every finite unsolvable group has a GRR [4].

In contrast to unrestricted GRRs, the question of whether a group has a GRR of prescribed valency is largely open. Research on this subject have been focusing on small valencies [3,5,8]. In 2002, Fang, Li, Wang and Xu [3] issued the following conjecture.

Conjecture 1.1 ([3, Remarks on Theorem 1.3]). *Every finite nonabelian simple group has a cubic GRR.*

Note that any GRR of a finite simple group must be connected, for otherwise its full automorphism group would be a wreath product. Hence if $\mathrm{Cay}(G, S)$ is a GRR of a finite simple group G, then S is necessarily a generating set of G. Apart from a few small groups, Conjecture 1.1 was only known to be true for the alternating groups [5] and Suzuki groups [3], while no counterexample was found yet. In this paper, we study cubic GRRs for finite projective special linear groups of dimension two. In particular, Theorem 1.3 shows that Conjecture 1.1 fails for $\mathrm{PSL}_2(7)$ but holds for all $\mathrm{PSL}_2(q)$ with $q \neq 7$.

For any subset S of a group G, denote by $\mathrm{Aut}(G, S)$ the group of automorphisms of G fixing S setwise. Each element in $\mathrm{Aut}(G, S)$ is an automorphism of $\mathrm{Cay}(G, S)$ fixing the identity of G. Hence a necessary condition for $\mathrm{Cay}(G, S)$ to be a GRR of G is that $\mathrm{Aut}(G, S) = 1$. In [3], the authors showed that this condition is also sufficient for many cubic Cayley graphs of finite simple groups. We state their result for simple groups $\mathrm{PSL}_2(q)$ as follows, which is the starting point of the present paper.

* Corresponding author.
E-mail addresses: binzhouxia@pku.edu.cn (B. Xia), tengfang@pku.edu.cn (T. Fang).

http://dx.doi.org/10.1016/j.disc.2016.03.008
0012-365X/

Theorem 1.2 *([3]). Let $G = \mathrm{PSL}_2(q)$ be a simple group, where $q \neq 11$ is a prime power, and S be a generating set of G with $S^{-1} = S$ and $|S| = 3$. Then $\mathrm{Cay}(G, S)$ is a GRR of G if and only if $\mathrm{Aut}(G, S) = 1$.*

The following are our three main results.

Theorem 1.3. *For any prime power $q \geqslant 5$, $\mathrm{PSL}_2(q)$ has a cubic GRR if and only if $q \neq 7$.*

Theorem 1.4. *For each prime power q there exist involutions x and y in $\mathrm{PSL}_2(q)$ such that the probability for a randomly chosen involution z to make*

$$\mathrm{Cay}(\mathrm{PSL}_2(q), \{x, y, z\})$$

a cubic GRR of $\mathrm{PSL}_2(q)$ tends to 1 as q tends to infinity.

Proposition 1.5. *Let $q \geqslant 5$ be a prime power and $G = \mathrm{PSL}_2(q)$. If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S is a set of three involutions.*

Theorem 1.4 shows that it is easy to make GRRs for $\mathrm{PSL}_2(q)$ from three involutions. On the other hand, Proposition 1.5 says that one can only make GRRs for $\mathrm{PSL}_2(q)$ from three involutions, which is a response to [5, Problem 1.2] as well. (Note that for a cubic Cayley graph $\mathrm{Cay}(G, S)$, the set S either consists of three involutions, or has the form $\{x, y, y^{-1}\}$ with $o(x) = 2$ and $o(y) > 2$.) The proof of Theorem 1.4 is at the end of Section 3, and the proofs of Theorem 1.3 and Proposition 1.5 are in Section 4. We also pose two problems concerning cubic GRRs for other families of finite simple groups at the end of this paper.

2. Preliminaries

The following result is well known, see for example [7, II §7 and §8].

Lemma 2.1. *Let $q \geqslant 5$ be a prime power and $d = \gcd(2, q-1)$. Then $\mathrm{PGL}_2(q)$ has a maximal subgroup $M = \mathrm{D}_{2(q+1)}$. Moreover, $M \cap \mathrm{PSL}_2(q) = \mathrm{D}_{2(q+1)/d}$, and for $q \notin \{7, 9\}$ it is maximal in $\mathrm{PSL}_2(q)$.*

The next lemma concerns facts about involutions in two-dimensional linear groups which is needed in the sequel.

Lemma 2.2. *Let $q = p^f \geqslant 5$ for some prime p and $G = \mathrm{PSL}_2(q)$. Then the following hold.*

(a) *There is only one conjugacy class of involutions in G.*
(b) *For any involution g in G,*

$$\mathbf{C}_G(g) = \begin{cases} \mathrm{C}_2^f, & \text{if } p = 2, \\ \mathrm{D}_{q-1}, & \text{if } q \equiv 1 \pmod 4, \\ \mathrm{D}_{q+1}, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

(c) *If $p > 2$, then for any involution α in $\mathrm{PGL}_2(q)$, the number of involutions in $\mathbf{C}_G(\alpha)$ is at most $(q+3)/2$.*

Proof. Parts (a) and (b) can be found in [6, Lemma A.3]. To prove part (c), assume that $p > 2$ and α is an involution in $\mathrm{PGL}_2(q)$. By [6, Lemma A.3] we have $\mathbf{C}_G(\alpha) = \mathrm{D}_{q+\varepsilon}$ with $\varepsilon = \pm 1$. As a consequence, the number of involutions in $\mathbf{C}_G(\alpha)$ is at most $1 + (q+\varepsilon)/2 \leqslant (q+3)/2$. This completes the proof. □

3. GRRs from three involutions

Recall from Lemma 2.1 that $\mathrm{PSL}_2(q)$ has a maximal subgroup $\mathrm{D}_{2(q+1)/d}$, where $d = \gcd(2, q-1)$. The following proposition plays the central role in this paper.

Proposition 3.1. *Let $q = p^f \geqslant 11$ for some prime p, $d = \gcd(2, q-1)$, $G = \mathrm{PSL}_2(q)$, and $H = \mathrm{D}_{2(q+1)/d}$ be a maximal subgroup of G. Then for any two involutions x, y with $\langle x, y\rangle = H$, there are at least*

$$\frac{q^2 - 4d^2fq - (d+2)q - 4d^2f - 3d^2 + 2d - 1}{d}$$

involutions $z \in G$ such that $\langle x, y, z\rangle = G$ and $\mathrm{Aut}(G, \{x, y, z\}) = 1$.

Proof. Fix involutions x, y in H such that $\langle x, y\rangle = H$. Identify the elements in G with their induced inner automorphisms of G. In this way, G is a normal subgroup of $A := \mathrm{Aut}(G)$, and the elements of A act on G by conjugation. Denote by V the set of involutions in G, and

$$L = \{y^\alpha \mid \alpha \in A, x^\alpha = x\} \cup \{y^\alpha \mid \alpha \in A, x^\alpha = y\} \cup \{x^\alpha \mid \alpha \in A, y^\alpha = x\} \cup \{x^\alpha \mid \alpha \in A, y^\alpha = y\}.$$