Oriented regular representations of out-valency two for finite simple groups[*]

Gabriel Verret [iD]

Department of Mathematics, University of Auckland, PB 92019, Auckland, New Zealand

Binzhou Xia [†] [iD]

School of Mathematics and Statistics, University of Melbourne,
Parkville, VIC 3010, Australia

Abstract

In this paper, we show that every finite simple group of order at least 5 admits an oriented regular representation of out-valency 2.

Keywords: Finite simple group, DRR, ORR.

Math. Subj. Class. (2020): 05C25, 05C20, 20B25

1 Introduction

All groups and digraphs in this paper are finite. A *digraph* Γ consists of a set of vertices $V(\Gamma)$ and a set of arcs $A(\Gamma)$, each arc being an ordered pair of vertices. A digraph is *proper* if (u, v) being an arc implies that (v, u) is not an arc. The automorphisms of Γ are the permutations of $V(\Gamma)$ that preserve $A(\Gamma)$. Under composition, they form the automorphism group $\mathrm{Aut}(\Gamma)$ of Γ.

Let G be a group and $S \subseteq G$. The *Cayley digraph* $\mathrm{Cay}(G, S)$ on G with connection set S is the digraph with vertex set G and (u, v) being an arc whenever $vu^{-1} \in S$. Note that $\mathrm{Cay}(G, S)$ is a proper digraph if and only if $S \cap S^{-1} = \emptyset$. Note also that every vertex u in $\mathrm{Cay}(G, S)$ is contained in exactly $|S|$ arcs of the form (u, v). We thus say that $\mathrm{Cay}(G, S)$ has *out-valency* $|S|$.

It is easy to see that $\mathrm{Aut}(\mathrm{Cay}(G, S))$ contains the right regular representation of G. If this containment is actually equality, then $\mathrm{Cay}(G, S)$ is called a *digraphical regular*

[†]Corresponding author.
E-mail addresses: g.verret@auckland.ac.nz (Gabriel Verret), binzhoux@unimelb.edu.au (Binzhou Xia)

representation (or DRR) of G. A DRR that is a proper digraph is called an *oriented regular representation* (or ORR).

Babai proved that, apart from five small groups, all groups admit a DRR [1, Theorem 2.1]. He also asked which groups admit ORRs [1, Problem 2.7]. This was answered by Morris and Spiga [9, 10, 12] who showed that apart from generalised dihedral groups and a small list of exceptions, all groups admit ORRs.

In view of the above, a natural problem is to find "nice" DRRs and ORRs, say of "small" out-valency. Clearly, only cyclic groups can have DRRs of out-valency 1, so out-valency 2 is the smallest interesting case. In this paper, we give the most satisfactory answer to this question in the case of simple groups.

Theorem 1.1. *Every finite simple group of order at least* 5 *has a ORR of out-valency* 2.

A corollary of Theorem 1.1 is that every nonabelian simple group has a DRR of out-valency 2. However, the latter conclusion is an immediate consequence of the fact that every nonabelian simple group is generated by an involution and a non-involution (even by an involution and an element of odd prime order, see [8, Theorem 1]. Indeed, consider a Cayley digraph on a nonabelian simple group with connection set consisting of such a generating pair. This digraph has out-valency 2, but one out-neighbour of every vertex is also an in-neighbour while the other out-neighbour is not. This implies that fixing a vertex must also fix its out-neighbours and, by connectedness, the whole digraph, and the digraph is a DRR.

Note that Cayley digraphs of out-valency two of simple groups were previously studied in [4]. Another interesting variant of this question would be to consider undirected graphs. In this case, the smallest interesting valency is 3. The question of which simple groups admit graphical regular representations of valency 3 has received some attention but is still open [11, 13, 14, 15].

2 Preliminaries

2.1 Generation of finite simple groups

In this section we present some generation properties of finite simple groups, which will be needed in the proof of Theorem 1.1. The following result is due to Guralnick and Kantor [7, Corollary].

Theorem 2.1 (Guralnick-Kantor). *Every nontrivial element of a finite simple group belongs to a pair of elements generating the group.*

Note that Theorem 2.1 depends on the classification of finite simple groups.

Corollary 2.2. *Let G be a finite nonabelian simple group with an element x of order* 3. *Then there exists $y \in G$ such that $|y| \geq 4$ and $G = \langle x, y \rangle$.*

Proof. By Theorem 2.1 there exists $z \in G$ such that $G = \langle x, z \rangle$. Note that $\langle x, z \rangle = \langle x, xz \rangle$ hence, if either z or xz has order at least 4, then the conclusion holds (by taking $y = z$ or $y = xz$). We may thus assume that z and xz both have order at most 3. This implies that G is a quotient of the finitely presented group

$$\langle x, z \mid x^3, z^m, (xz)^n \rangle$$

with $m, n \leq 3$. This is the "ordinary" $(3, m, n)$ triangle group which is well known to be solvable when $m, n \leq 3$ (see for example [3]) and therefore so is G, which is a contradiction. $\qquad\square$

The only nonabelian simple groups with no elements of order 3 are the Suzuki groups (see [6, Page 8, Table I]), which we now consider. For a positive integer m and prime number p, a prime number r is called a *primitive prime divisor* of $p^m - 1$ if r divides $p^m - 1$ but does not divide $p^k - 1$ for any positive integer $k < m$. By Zsigmondy's theorem [17], $p^m - 1$ has a primitive prime divisor whenever $m \geq 3$ and $(p, m) \neq (2, 6)$.

Proposition 2.3. *Let $G = \mathrm{Sz}(q)$ with $q = 2^{2n+1} \geq 8$ and let r be a primitive prime divisor of $q^4 - 1$. Then $r \geq 5$, G has an element y of order r and, for each such y, there exists $x \in G$ such that $|x| = 4$, $|xy| \geq 3$ and $G = \langle x, y \rangle$.*

Proof. First, recall that $|G| = q^2(q^2 + 1)(q - 1)$ (see [6, Page 8, Table I]). Since r is a primitive prime divisor of $q^4 - 1$, it divides $q^4 - 1$ but not $q^2 - 1$ and thus must divide $q^2 + 1$. It follows that G has an element y of order r and that $r \geq 5$. We will now prove that there exists an element x of order 4 with the required properties, essentially by a somewhat crude counting argument.

We denote by E_q the elementary abelian group of order q and, for an integer $n \geq 2$, by C_n the cyclic group of order n and D_{2n} the dihedral group of order $2n$.

Up to conjugation, the maximal subgroups of G are the following (see for instance [2, Table 8.16]):

- $(\mathrm{E}_q.\mathrm{E}_q) \rtimes \mathrm{C}_{q-1}$,
- $\mathrm{D}_{2(q-1)}$,
- $\mathrm{C}_{q+\sqrt{2q}+1} \rtimes \mathrm{C}_4$,
- $\mathrm{C}_{q-\sqrt{2q}+1} \rtimes \mathrm{C}_4$,
- $\mathrm{Sz}(q_0)$, where $q_0 = q^{1/d} > 2$ for some prime divisor d of $2n + 1$.

Recall that r is odd, does not divide $q - 1$ nor $q_0^4 - 1$ and thus does not divide its factor $(q_0^2 + 1)(q_0 - 1)$. This implies that r does not divide $|\mathrm{Sz}(q_0)| = q_0^2(q_0^2 + 1)(q_0 - 1)$. It follows that a maximal subgroup M of G containing y must be of the form $\mathrm{C}_{q\pm\sqrt{2q}+1} \rtimes \mathrm{C}_4$. Since every subgroup of a cyclic group is characteristic, $\langle y \rangle$ is normal in M and thus M is the only maximal subgroup of G containing y (for otherwise $\langle y \rangle$ would be normal in another maximal subgroup N of G and thus normal in $\langle M, N \rangle = G$).

Let Q be a Sylow 2-subgroup of G. Then $Q = \mathrm{E}_q.\mathrm{E}_q$ and $|\mathbf{N}_G(Q)| = (\mathrm{E}_q.\mathrm{E}_q) \rtimes \mathrm{C}_{q-1}$. Hence the number n of Sylow 2-subgroups of G is

$$n = \frac{|G|}{|\mathbf{N}_G(Q)|} = \frac{q^2(q^2 + 1)(q - 1)}{q^2(q - 1)} = q^2 + 1.$$

Let n_2 and n_4 denote the numbers of elements of order 2 and 4, respectively, in G. According to [5, Lemma 3.2], there are $q - 1$ involutions and $q^2 - q$ elements of order 4 in Q, and different conjugates of Q have trivial intersection. Then

$$n_2 = n(q - 1) = (q^2 + 1)(q - 1)$$

and

$$n_4 = n(q^2 - q) = (q^2 + 1)(q^2 - q).$$

Let

$$I = \{g \in G : |gy| \leq 2\}$$

and

$$J = \{g \in G : \langle g, y \rangle \neq G\}.$$

Then $|I| = n_2 + 1$ and, since M is the unique maximal subgroup of G containing y, $|J| \leq |M|$. Since

$$
\begin{aligned}
|I| + |J| &\leq n_2 + |M| + 1 \\
&= (q^2 + 1)(q - 1) + 4(q \pm \sqrt{2q} + 1) + 1 \\
&\leq (q^2 + 1)(q - 1) + 4(q + \sqrt{2q} + 1) + 1 \\
&< (q^2 + 1)(q^2 - q) = n_4,
\end{aligned}
$$

it follows that there exists $x \in G$ with $|x| = 4$ and $x \notin I \cup J$, as required. $\qquad\square$

2.2 Constructing ORRs of out-valency 2

Lemma 2.4. *Let $G = \langle x, y \rangle$. If $|x| = 3$ and $|y| \geq 4$, then $\mathrm{Cay}(G, \{x, y\})$ is an ORR, unless $|y| = 6$ and $x = y^4$, and $G \cong \mathrm{C}_6$.*

Proof. Let $\Gamma = \mathrm{Cay}(G, \{x, y\})$ and let $A = \mathrm{Aut}(\Gamma)$. Note that Γ is a strongly connected proper digraph. Figure 1 shows all the directed paths of length at most 3 in Γ starting at 1.
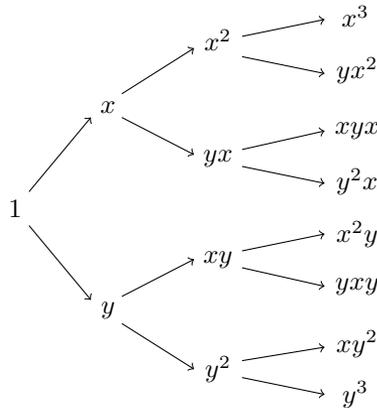

Figure 1: All the directed paths of length at most 3 in $\mathrm{Cay}(G, \{x, y\})$.

Since $|y| \geq 4$, we have $y^3 \neq 1$ and $y \neq x^{-2}$. Moreover, if $y^2 = x^{-1}$, then $|y| = 6$ and thus $x = y^4$ and the result holds. We thus assume this is not the case. Since $x^3 = 1$, this implies that $(1, x, x^2, x^3)$ is the only directed cycle of length 3 starting at 1. This implies that the stabiliser A_1 of the vertex 1 also fixes x. As 1 only has one out-neighbour other than x, it must also be fixed. By vertex-transitivity, we find that fixing a vertex fixes its out neighbours and, using connectedness, we conclude that $A_1 = 1$ and thus Γ is an ORR. $\quad\square$

Lemma 2.5. *Let $G = \langle x, y \rangle$. If $|x| = 4$, $|y| \geq 5$ and $|xy| \geq 3$, then $\mathrm{Cay}(G, \{x, y\})$ is an ORR, unless $|y| = 12$ and $x = y^9$, and $G \cong \mathrm{C}_{12}$.*

Proof. Let $\Gamma = \mathrm{Cay}(G, \{x, y\})$ and let $A = \mathrm{Aut}(\Gamma)$. Note that Γ is a strongly connected proper digraph. Figure 2 shows all the directed paths of length at most 4 in Γ starting at 1.
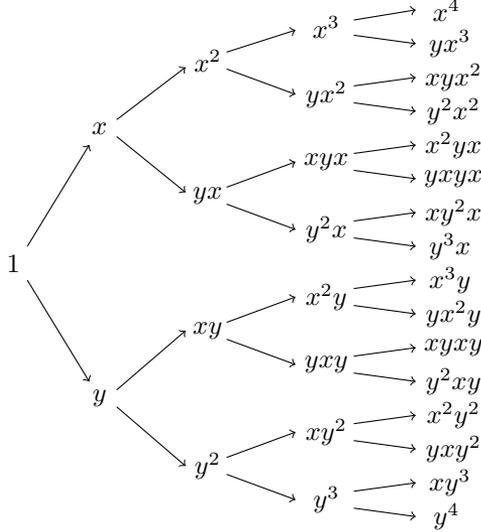

Figure 2: All the directed paths of length at most 4 in $\mathrm{Cay}(G, \{x, y\})$.

Since $|y| \geq 5$, we have $y^4 \neq 1$, $y \neq x^{-3}$ and $y^2 \neq x^{-2}$. Similarly, $|xy| \geq 3$ implies that $(xy)^2 \neq 1 \neq (yx)^2$. Moreover, if $y^3 = x^{-1}$, then $|y| = 12$ and thus $x = y^9$ and the result holds. We thus assume this is not the case. Since $x^4 = 1$, this implies that $(1, x, x^2, x^3, x^4)$ is the only directed cycle of length 4 starting at 1 and, as in the previous lemma, Γ is an ORR. □

3 Proof of Theorem 1.1

Let G be a finite simple group with $|G| \geq 5$. We first suppose that $G = \mathbb{F}_p^+$ for some prime $p \geq 5$. Let $x, y \in \mathbb{F}_p \setminus \{0\}$ such that $x \neq \pm y$ and let $\Gamma = \mathrm{Cay}(G, \{x, y\})$. Note that Γ is a proper digraph of out-valency 2. By [16, Proposition 1.3 and Example 2.2], Γ is an ORR if and only if the only solution to

$$\{\lambda x, \lambda y\} = \{x, y\} \tag{3.1}$$

with $\lambda \in \mathbb{F}_p^\times$ is $\lambda = 1$. Suppose otherwise, that is (3.1) holds with $\lambda \neq 1$. This implies that $\lambda x = y$ and $\lambda y = x$, which yields that

$$\lambda x^2 = (\lambda x)x = y(\lambda y) = \lambda y^2,$$

and hence $x^2 = y^2$, contradicting $x \neq \pm y$. Thus we conclude that Γ is an ORR, as required.

We may now assume that G is nonabelian. If G has an element x of order 3 then, by Corollary 2.2 there exists $y \in G$ such that $|y| \geq 4$ and $G = \langle x, y \rangle$. By Lemma 2.4, $\mathrm{Cay}(G, \{x, y\})$ is an ORR. We may thus assume that G does not have an element of order

3 and thus $G = \mathrm{Sz}(q)$ for some $q = 2^{2n+1} \geq 8$. Let r be a primitive prime divisor of $q^4 - 1$. By Proposition 2.3, G contains elements x and y such that $|x| = 4$, $|y| = r \geq 5$, $|xy| \geq 3$ and $G = \langle x, y \rangle$. By Lemma 2.5, $\mathrm{Cay}(G, \{x, y\})$ is an ORR. $\square$

ORCID iDs

Gabriel Verret ⓘ https://orcid.org/0000-0003-1766-4834
Binzhou Xia ⓘ https://orcid.org/0000-0002-8031-2981

References

[1] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* **11** (1980), 257–270, doi:10.1007/bf02107568.

[2] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, volume 407 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2013, doi:10.1017/cbo9781139192576.

[3] M. D. E. Conder, Some results on quotients of triangle groups, *Bull. Austral. Math. Soc.* **30** (1984), 73–90, doi:10.1017/s0004972700001738.

[4] X.-G. Fang, Z.-P. Lu, J. Wang and M.-Y. Xu, Cayley digraphs of finite simple groups with small out-valency, *Comm. Algebra* **32** (2004), 1201–1211, doi:10.1081/agb-120027974.

[5] X. G. Fang and C. E. Praeger, Finite two-arc transitive graphs admitting a Suzuki simple group, *Comm. Algebra* **27** (1999), 3727–3754, doi:10.1080/00927879908826659.

[6] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups*, volume 40 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, 1994, doi:10.1090/surv/040.1.

[7] R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), 743–792, doi:10.1006/jabr.2000.8357.

[8] C. S. H. King, Generation of finite simple groups by an involution and an element of prime order, *J. Algebra* **478** (2017), 153–173, doi:10.1016/j.jalgebra.2016.12.031.

[9] J. Morris and P. Spiga, Every finite non-solvable group admits an oriented regular representation, *J. Comb. Theory Ser. B* **126** (2017), 198–234, doi:10.1016/j.jctb.2017.05.003.

[10] J. Morris and P. Spiga, Classification of finite groups that admit an oriented regular representation, *Bull. Lond. Math. Soc.* **50** (2018), 811–831, doi:10.1112/blms.12177.

[11] P. Spiga, Cubic graphical regular representations of finite non-abelian simple groups, *Comm. Algebra* **46** (2018), 2440–2450, doi:10.1080/00927872.2017.1383997.

[12] P. Spiga, Finite groups admitting an oriented regular representation, *J. Comb. Theory Ser. A* **153** (2018), 76–97, doi:10.1016/j.jcta.2017.08.001.

[13] B. Xia, Cubic graphical regular representations of $\mathrm{PSL}_3(q)$, *Discrete Math.* **343** (2020), 111646 (9 pages), doi:10.1016/j.disc.2019.111646.

[14] B. Xia, On cubic graphical regular representations of finite simple groups, *J. Comb. Theory Ser. B* **141** (2020), 1–30, doi:10.1016/j.jctb.2019.06.002.

[15] B. Xia and T. Fang, Cubic graphical regular representations of $\mathrm{PSL}_2(q)$, *Discrete Math.* **339** (2016), 2051–2055, doi:10.1016/j.disc.2016.03.008.

[16] M.-Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319, doi:10.1016/s0012-365x(97)00152-0.

[17] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284, doi:10.1007/bf01692444.