THE ART OF DISCRETE AND APPLIED MATHEMATICS

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 4 (2021) #P1.10
https://doi.org/10.26493/2590-9770.1338.0b2
(Also available at http://adam-journal.eu)

On the equivalence between a conjecture of Babai-Godsil and a conjecture of Xu concerning the enumeration of Cayley graphs

Pablo Spiga

Pablo Spiga,Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca Via Cozzi 55, 20125 Milano, Italy

Received 20 November 2019, accepted 12 October 2020, published online 01 April 2021

Abstract

In this paper we show that two distinct conjectures, the first proposed by Babai and Godsil in 1982 and the second proposed by Xu in 1998, concerning the asymptotic enumeration of Cayley graphs are in fact equivalent. This result follows from a more general theorem concerning the asymptotic enumeration of a certain family of Cayley graphs.

Keywords: Regular representation, Cayley graph, automorphism group, asymptotic enumeration, graphical regular representation, GRR, normal Cayley graph, Babai-Godsil conjecture, Xu conjecture.

Math. Subj. Class.: 05C25, 05C30, 20B25, 20B15

1 Introduction

All digraphs and groups considered in this paper are finite. A ***digraph*** Γ is an ordered pair (V, A) where the ***vertex-set*** V is a finite non-empty set and the ***arc-set*** $A \subseteq V \times V$ is a binary relation on V. The elements of V and A are called ***vertices*** and ***arcs*** of Γ, respectively. An ***automorphism*** of Γ is a permutation σ of V with $A^\sigma = A$, that is, $(x^\sigma, y^\sigma) \in A$ for every $(x, y) \in A$. Let R be a group and let S be a subset of R. The ***Cayley digraph*** on R with connection set S (which we denote by $\Gamma(R, S)$) is the digraph with vertex-set R and with (g, h) being an arc if and only if $hg^{-1} \in S$. The group R acts regularly as a group of automorphisms of $\Gamma(R, S)$ by right multiplication and hence $R \leq \mathrm{Aut}(\Gamma(R, S))$. When $R = \mathrm{Aut}(\Gamma(R, S))$, the digraph Γ is called a ***DRR*** (for digraphical regular representation). Babai and Godsil made the following conjecture.

E-mail address: pablo.spiga@unimib.it (Pablo Spiga)

Conjecture 1.1 ([6, Conjecture 3.13], [2]). *Let R be a group of order r. The proportion of subsets S of R such that $\Gamma(R,S)$ is a* DRR *goes to* 1 *as $r \to \infty$. More precisely,*

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : \mathrm{Aut}(\Gamma(R,S)) = R\}|}{2^r} : |R| = r \right\} = 1.$$

This conjecture has been recently proved in [12].

This paper is the first step for proving yet another conjecture of Babai and Godsil concerning the enumeration of ***Cayley graphs***. A Cayley graph over R is a Cayley digraph $\Gamma(R,S)$ whose binary relation $\{(g,h) \in R \times R \mid gh^{-1} \in S\}$ defining the arc-set of $\Gamma(R,S)$ is symmetric. (Incidentally, the binary relation $\{(g,h) \in R \times R \mid gh^{-1} \in S\}$ is riflexive if and only if S contains the identity element of G.) In terms of the connection set $S \subseteq R$, $\Gamma(R,S)$ is a Cayley graph if and only if $S = S^{-1}$, where $S^{-1} := \{s^{-1} \mid s \in S\}$. Given a subset S of R, we say that S is ***inverse-closed*** if $S = S^{-1}$, that is, $\Gamma(R,S)$ is undirected, which in turn means that $\Gamma(R,S)$ is a Cayley graph. When $R = \mathrm{Aut}(\Gamma(R,S))$ and S is inverse-closed, the graph Γ is called a ***GRR*** (for graphical regular representation).

While the number of Cayley digraphs on R is $2^{|R|}$, which is a number that depends on the cardinality of R only, the number of undirected Cayley graphs on R is $2^{\frac{|R|+|\mathbf{I}(R)|}{2}}$ (see Lemma 2.2), where $\mathbf{I}(R) := \{\iota \in R \mid \iota^2 = 1\}$, and hence depends on the algebraic structure of R.

Although the difference between Cayley digraphs and Cayley graphs seems only minor and to some extent only aesthetic, the behaviour between these two classes of combinatorial objects with respect to their automorphisms can be dramatically different. For instance, it was proved by Babai [1, Theorem 2.1] that, except for

$$Q_8,\ C_2 \times C_2,\ C_2 \times C_2 \times C_2,\ C_2 \times C_2 \times C_2 \times C_2 \text{ and } C_3 \times C_3,$$

every finite group R admits a DRR. Borrowing a phrase which I once heard from Tom Tucker: "Besides some low level noise, every finite group admits a DRR". The analogue for GRRs is not the same. Indeed, it turns out that there are two (and only two) infinite families of groups that do no admit GRRs. The first family consists of abelian groups of exponent greater than two. If R is such a group and ι is the automorphism of R mapping every element to its inverse, then every Cayley graph on R admits $R \rtimes \langle\iota\rangle$ as a group of automorphisms. Since R has exponent greater than 2, $\iota \neq 1$ and hence no Cayley graph on R is a GRR. The other family of groups that do not admit GRRs are the generalised dicyclic groups, see [14, Definition 1.1] for a definition and also Definition 2.4 below. These two families were discovered by Mark Watkins [19].

It was proved by Godsil [5] that abelian groups of exponent greater than 2 and generalised dicyclic groups are the only two infinite families of groups that do not admit GRRs. (A lot of papers have been published for determining those groups admitting a GRR, and some of the most influential works along the way appeared in [7, 8, 9, 15, 16, 20].) The stronger Conjecture 1.2 was made (at various times) by Babai, Godsil, Imrich and Lovász.

Conjecture 1.2 (see [2, Conjecture 2.1] and [6, Conjecture 3.13]). *Let R be a group of order r which is neither generalized dicyclic nor abelian of exponent greater than* 2*. The proportion of inverse-closed subsets S of R such that $\Gamma(R,S)$ is a* GRR *goes to* 1 *as $r \to \infty$. More precisely,*

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : \mathrm{Aut}(\Gamma(R,S)) = R\}|}{2^{\mathbf{c}(R)}} : R \text{ admits a GRR and } |R| = r \right\} = 1.$$

This conjecture is open at the moment and some of the techniques developed in [12] for dealing with digraphs are not suited for dealing with undirected graphs.

The scope of this paper is twofold. Broadly speaking, we aim to start a long process where we try to generalize and adapt the results obtained in [12] for eventually dealing with undirected graphs and proving Conjecture 1.2. Given an inverse-closed subset S of R, we let $A := \mathrm{Aut}(\Gamma(R,S))$. Now, the set S fails to give rise to a GRR essentially for two different reasons.

1. There are non-identity group automorphisms of R leaving the set S invariant. This case arises when $\mathbf{N}_A(R) > R$ (this is the typical obstruction and we have encountered this obstruction already when we briefly discussed abelian groups of exponent greater than 2).
2. The only group automorphism of R leaving the set S invariant is the identity and there are some automorphisms of $\Gamma(R,S)$ not lying in R. This case arises when $\mathbf{N}_A(R) = R$ and $A > R$: this obstruction is somehow mysterious and much harder to analyze.

These two obstructions are clear (if not obvious) to readers familiar with the enumeration problem of Cayley graphs [12] and in particular to readers familiar with [2]. Actually the same obstructions arise in the enumeration problem of other types of Cayley graphs, for instance in the asymptotic enumeration of DFRs [17] and GFRs [4, 18] and in the recent solution of the GFR conjecture [18]. We start this process by dealing with the ***first natural obstruction*** for the existence of GRRs.[1]

Theorem 1.3. *Let R be a group of order r which is neither generalized dicyclic nor abelian of exponent greater than 2. The proportion of inverse-closed subsets S of R such that $\mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R) > R$ goes to 0 as $r \to \infty$.*

We observe that in Proposition 2.9 we have a quantified version of Theorem 1.3. Moreover, in Lemma 2.8 we have a more technical version of Theorem 1.3 which includes also generalized dicyclic groups and abelian groups of exponent greater than 2. These two more technical results are in our opinion needed to follow the footsteps of the argument in [12] for the asymptotic enumeration of Cayley digraphs.

The second scope of this paper is to prove that a famous conjecture of Xu on the asymptotic enumeration of normal Cayley graphs is actually equivalent to Conjecture 1.2. A Cayley (di)graph Γ on R is said to be a ***normal Cayley (di)graph on*** R if the regular representation of R is normal in $\mathrm{Aut}(\Gamma)$, that is, $R \trianglelefteq \mathrm{Aut}(\Gamma)$. Clearly, every DRR and every GRR Γ on R is a normal Cayley (di)graph because $R = \mathrm{Aut}(\Gamma)$. Xu has conjectured that almost all Cayley (di)graphs on R are normal Cayley (di)graphs on R. Indeed, Xu in [21] has posed the following two conjectures.

Conjecture 1.4 (see [21])**.** *The minimum, over all groups R of order r, of the proportion of subsets S of R such that $\Gamma(R,S)$ is a normal Cayley graph tends to 1 as $r \to \infty$. More precisely,*

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : R \trianglelefteq \mathrm{Aut}(\Gamma(R,S))\}|}{2^r} : |R| = r \right\} = 1.$$

[1] During the refereeing process of this paper a substantial step towards the second obstruction has been obtained in [13]

Conjecture 1.5 (see [21]). *The minimum, over all groups R of order r, of the proportion of inverse-closed subsets S of R such that $\Gamma(R,S)$ is a normal Cayley graph tends to 1 as $r \to \infty$. More precisely,*

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : R \trianglelefteq \mathrm{Aut}(\Gamma(R,S))\}|}{2^{\mathbf{c}(R)}} : |R| = r \right\} = 1.$$

Conjecture 1.4 was shown to be true in [12] by proving the stronger Conjecture 1.1. The veracity of Conjecture 1.5 when R is an abelian group and when R is a dicyclic group was proved in [3, 14]. In this paper we show that Conjecture 1.2 and Conjecture 1.5 are actually equivalent.

Theorem 1.6. *Conjecture 1.2 holds true if and only if Conjecture 1.5 holds true.*

2 Group automorphisms

Definition 2.1. Given a finite group R and $x \in R$, we let $o(x)$ denote the order of the element x and we let $\mathbf{I}(R) := \{x \in R \mid o(x) \leq 2\}$ be the set of elements of R having order at most 2. We let $\mathbf{c}(R)$ denote the fraction $(|R| + |\mathbf{I}(R)|)/2$, that is,

$$\mathbf{c}(R) = \frac{|R| + |\mathbf{I}(R)|}{2}.$$

Given a subset X of R, we write $\mathbf{I}(X) := X \cap \mathbf{I}(R)$. Finally, we denote by $\mathbf{Z}(R)$ the centre of R.

Lemma 2.2. *Let R be a finite group. The number of inverse-closed subsets S of R is $2^{\mathbf{c}(R)}$.*

Proof. Given an arbitrary inverse-closed subset S of R, $S \cap \mathbf{I}(R)$ is an arbitrary subset of $\mathbf{I}(R)$ whereas in $S \cap (R \setminus \mathbf{I}(R))$ the elements come in pairs, where each element is paired up to its inverse. Thus the number of inverse-closed subsets of R is

$$2^{|\mathbf{I}(R)|} \cdot 2^{\frac{|R\setminus\mathbf{I}(R)|}{2}} = 2^{\mathbf{c}(R)}. \quad \square$$

Definition 2.3. Let R be a finite group. Given an automorphism φ of R, we set

$$\mathbf{C}_R(\varphi) := \{x \in R \mid x^\varphi = x\},$$
$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} := \{x \in R \mid x^\varphi = x^{-1}\}.$$

Observe that, when $\varphi = id_R$ is the identity automorphism of R, $\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(R)$.

Given $x \in R$, we denote by $\iota_x : R \to R$ the inner automorphism of R induced by x, that is, $m^{\iota_x} = xmx^{-1}$, for every $m \in R$. (Usually, the automorphism ι_x is defined by $m \mapsto m^{\iota_x} = x^{-1}mx$, however for our application it is more convenient to define ι_x by $m \mapsto m^{\iota_x} = xmx^{-1}$.) When $A \trianglelefteq R$, we still denote by ι_x the restriction to A of the automorphism ι_x, this makes the notation not too cumbersome to use and hopefully will cause no confusion.

Finally, we let $\iota : R \to R$ be the permutation defined by $x^\iota = x^{-1}$, for every $x \in R$. In particular, when R is abelian, ι is an automorphism of R. Furthermore, $\iota = id_R$ if and only if R is an abelian group of exponent at most 2.

Definition 2.4. Let A be an abelian group of even order and of exponent greater than 2, and let y be an involution of A. The *generalised dicyclic group* $\mathrm{Dic}(A,y,x)$ is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A\rangle$. A group is called *generalised dicyclic* if it is isomorphic to some $\mathrm{Dic}(A,y,x)$. When A is cyclic, $\mathrm{Dic}(A,y,x)$ is called a *dicyclic* or *generalised quaternion group*.

We let $\bar\iota_A : \mathrm{Dic}(A,y,x) \to \mathrm{Dic}(A,y,x)$ be the mapping defined by $(ax)^{\bar\iota_A} = ax^{-1}$ and $a^{\bar\iota_A} = a$, for every $a \in A$. In particular, $\bar\iota_A$ is an automorphism of $\mathrm{Dic}(A,y,x)$. The role of the label "A" in $\bar\iota_A$ seems unnecessary, however we use this label to stress one important fact. An abstract group R might be isomorphic to $\mathrm{Dic}(A,y,x)$, for various choices of A. Therefore, since the automorphism $\bar\iota_A$ depends on A and since we might have more than one choice of A, we prefer a notation that emphasizes this fact.

Lemma 2.5. *Let R be a finite group and let φ be an automorphism of R with $|R : \mathbf{C}_R(\varphi)| = 2$. Then one of the following holds:*

1. $\frac{1}{4}(|R| + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|) \le \mathbf{c}(R) - \frac{|R|}{32}$,
2. *R is generalized dicyclic over the abelian group $\mathbf{C}_R(\varphi)$ and $\varphi = \bar\iota_{\mathbf{C}_R(\varphi)}$,*
3. *R is abelian of exponent greater than 2 and $\varphi = \iota$.*

Proof. For simplicity, we let $A := \mathbf{C}_R(\varphi)$ and we let o denote the left-hand side in (1).

Suppose that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \subseteq A$. Then

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A = \{a \in A \mid a^\varphi = a^{-1}\} = \mathbf{C}_A(\varphi)^{\mathrm{inv}}.$$

Since $A = \mathbf{C}_R(\varphi)$, we have $a^\varphi = a$ for every $a \in A$ and hence

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{C}_A(\varphi)^{\mathrm{inv}} = \mathbf{C}_A(id_A)^{\mathrm{inv}}.$$

Clearly, $a \in \mathbf{C}_A(id_A)^{\mathrm{inv}}$ if and only if $a = a^{-1}$, that is, $a \in \mathbf{I}(A)$. Therefore

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{C}_A(\varphi)^{\mathrm{inv}} = \mathbf{C}_A(id_A)^{\mathrm{inv}} = \mathbf{I}(A).$$

Thus

$$\begin{aligned} o &= \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + \frac{|R|}{2} + |\mathbf{I}(A)|\right) \\ &\le \frac{1}{4}\left(\frac{3}{2}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{8} \\ &= \mathbf{c}(R) - \frac{|R|}{8}, \end{aligned}$$

and (1) holds in this case.

Suppose that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \not\subseteq A$. In particular, there exists $x \in R \setminus A$ with $x^\varphi = x^{-1}$. As $|R : A| = 2$, we have $R = A \cup Ax$. For every $a \in A$, since φ is an automorphism of R fixing point-wise A and since $xax^{-1} \in A$, we deduce

$$xax^{-1} = (xax^{-1})^\varphi = x^\varphi a^\varphi (x^{-1})^\varphi = x^{-1}ax$$

and hence $x^2a = ax^2$, that is, $x^2 \in \mathbf{Z}(\langle A, x\rangle) = \mathbf{Z}(R)$. As $x^2 \in A$, we have $x^2 = (x^2)^\varphi = (x^\varphi)^2 = (x^{-1})^2 = x^{-2}$, that is, $x^4 = 1$. Summing up,

$$x^2 \in \mathbf{Z}(R), \quad x^4 = 1. \tag{2.1}$$

Now, let $y \in \mathbf{C}_R(\varphi)^{\mathrm{inv}} \setminus A$. Then, $y = ax$, for some $a \in A$. Moreover, $y^\varphi = y^{-1} = (ax)^{-1} = x^{-1}a^{-1}$ and $y^\varphi = (ax)^\varphi = a^\varphi x^\varphi = ax^{-1}$. Thus

$$x^{-1}a^{-1} = ax^{-1},$$

that is, $xax^{-1} = a^{-1}$. Recall that $\iota_x : A \to A$ is the restriction to the normal subgroup A of the inner automorphism of R determined by x, that is, $a^{\iota_x} = xax^{-1}$, for every $a \in A$. We have shown that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \setminus A = \mathbf{C}_A(\iota_x)^{\mathrm{inv}}x$. As $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A = \mathbf{I}(A)$, we get

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(A) \cup \mathbf{C}_A(\iota_x)^{\mathrm{inv}}x \tag{2.2}$$

and $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = |\mathbf{I}(A)| + |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}|$.

Suppose that $|\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| \leq 3|A|/4$. Thus, by (2.2), we have

$$\begin{aligned} o &= \frac{1}{4}\left(\frac{3}{2}|R| + |\mathbf{I}(R)| + |\mathbf{I}(A)| + |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}|\right) \\ &\leq \frac{1}{4}\left(\frac{3}{2}|R| + 2|\mathbf{I}(R)| + \frac{3|A|}{4}\right) \\ &= \frac{1}{4}\left(\frac{3}{2}|R| + 2|\mathbf{I}(R)| + \frac{3|R|}{8}\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{32} \\ &= \mathbf{c}(R) - \frac{|R|}{32}, \end{aligned}$$

and (1) holds in this case.

Suppose that $|\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| > 3|A|/4$, that is, the automorphism ι_x of A inverts more than $3/4$ of its elements. By a result of Miller [11], A is abelian. Since A is abelian, it is easy to verify that $\mathbf{C}_A(\iota_x)^{\mathrm{inv}}$ is a subgroup of A. As $|\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| > 3|A|/4$, we get $\mathbf{C}_A(\iota_x)^{\mathrm{inv}} = A$ and ι_x acts on A inverting each of its elements. From (2.2), we have

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(A) \cup Ax. \tag{2.3}$$

If $\mathbf{I}(R) \subseteq \mathbf{I}(A)$, then no element in Ax is an involution and hence x has order 4 from (2.1). When A has exponent greater than 2, we deduce $R \cong \mathrm{Dic}(A, x^2, x)$ is a generalized dicyclic group over A, $\varphi = \bar{\iota}_A$ and (2) holds in this case. When A has exponent at most 2, we have $\mathbf{I}(A) = A$ and $\varphi = \iota$. Hence $\mathbf{I}(R) = A$, R is an abelian group of exponent greater than 2 and (3) holds in this case. Therefore, we may suppose $\mathbf{I}(R) \nsubseteq \mathbf{I}(A)$.

Let $x' \in \mathbf{I}(R) \setminus A$. Then, $x' = ax$, for some $a \in A$. Then $1 = x'^2 = (ax)^2 = axax = a(xax^{-1})x^2 = aa^{-1}x^2 = x^2$ and hence $x^2 = 1$. Now, for every $b \in A$, we have $(bx)^2 = bxbx = b(xbx^{-1}) = bb^{-1} = 1$. This shows $\mathbf{I}(R) \setminus A = Ax$. Therefore,

$\mathbf{I}(R) = \mathbf{I}(A) \cup Ax$ and hence $\mathbf{I}(R) = \mathbf{C}_R(\varphi)^{\mathrm{inv}}$ from (2.3). We deduce

$$\begin{aligned} o &= \frac{1}{4}\left(\frac{3|R|}{4} + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|\right) \\ &= \frac{1}{4}\left(\frac{3}{2}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{8} = \mathbf{c}(R) - \frac{|R|}{8}, \end{aligned}$$

and (1) holds in this case. □

Lemma 2.6. *Let R be a finite group and let φ be an automorphism of R with $|R : \mathbf{C}_R(\varphi)| = 3$. Then one of the following holds:*

1. $\frac{1}{4}(|R| + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|) \leq \mathbf{c}(R) - \frac{|R|}{96}$,
2. *R is abelian of exponent greater than 2 and $\varphi = \iota$.*

Proof. For simplicity, we let $A := \mathbf{C}_R(\varphi)$ and we let o denote the left-hand side in (1). As $|R : A| = 3$, we may write $R = A \cup Ax \cup Ax'$, for some $x, x' \in R$.

Suppose that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \subseteq A \cup Ay$, for some $y \in \{x, x'\}$. Then

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A) \cup (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ay) = \mathbf{I}(A) \cup (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ay) \subseteq \mathbf{I}(A) \cup Ay,$$

because φ fixes each element of A. Thus $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq |\mathbf{I}(R)| + |A|$ and

$$\begin{aligned} o &\leq \frac{1}{4}\left(\frac{4}{3}|R| + |\mathbf{I}(R)| + |\mathbf{I}(R)| + |A|\right) \\ &\leq \frac{1}{4}\left(\frac{4}{3}|R| + 2|\mathbf{I}(R)| + \frac{|R|}{3}\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{12} \\ &= \mathbf{c}(R) - \frac{|R|}{12}, \end{aligned}$$

and (1) holds in this case.

Therefore we may suppose that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ax \neq \emptyset$ and $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ax' \neq \emptyset$. In particular, replacing x and x' if necessary, we may suppose that $x, x' \in \mathbf{C}_R(\varphi)^{\mathrm{inv}}$, that is, $x^\varphi = x^{-1}$ and $x'^\varphi = x'^{-1}$.

CASE: $A \trianglelefteq R$.

As R/A is cyclic of order 3, we may assume that $x' = x^{-1}$ and that x has odd order. For every $a \in A$, we have $xax^{-1} \in A$ and hence

$$xax^{-1} = (xax^{-1})^\varphi = x^\varphi a^\varphi (x^{-1})^\varphi = x^{-1}ax,$$

that is, $x^2 a = ax^2$. Therefore $x^2 \in \mathbf{Z}(\langle x, A\rangle) = \mathbf{Z}(R)$. As x has odd order, we deduce $x \in \mathbf{Z}(R)$. From this it is easy to deduce that

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(A) \cup \mathbf{I}(A)x \cup \mathbf{I}(A)x^{-1}. \tag{2.4}$$

Assume that $|\mathbf{I}(A)| \leq 3|A|/4$. Thus, by (2.4), we have

$$\begin{aligned} o &= \frac{1}{4}\left(\frac{4}{3}|R| + |\mathbf{I}(R)| + |\mathbf{I}(A)| + |\mathbf{I}(A)| + |\mathbf{I}(A)|\right) \\ &\leq \frac{1}{4}\left(\frac{4}{3}|R| + 2|\mathbf{I}(R)| + 2|\mathbf{I}(A)|\right) \\ &\leq \frac{1}{4}\left(\frac{4}{3}|R| + 2|\mathbf{I}(R)| + 2\frac{3|A|}{4}\right) = \frac{1}{4}\left(\frac{4}{3}|R| + 2|\mathbf{I}(R)| + \frac{|R|}{2}\right) \\ &= \frac{1}{4}\left(\frac{11}{6}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{24} = \mathbf{c}(R) - \frac{|R|}{24}, \end{aligned}$$

and (1) holds in this case.

Assume that $|\mathbf{I}(A)| > 3|A|/4$. By [11], A is abelian. Thus $\mathbf{I}(A)$ is a subgroup of A with $|\mathbf{I}(A)| > 3|A|/4$. It follows that A is an elementary abelian 2-group. As $x \in \mathbf{Z}(R)$, we deduce that R is abelian and $\varphi = \iota$; thus (2) holds in this case.

CASE: A IS NOT NORMAL IN R.

Let K be the core of A in R. Observe that the group R acts on the right cosets of A in R. As $|R : A| = 3$, this action gives rise to a transitive permutation representation of R inside the symmetric group of degree 3. The kernel of this permutation representation is, by definition, K and hence R/K is isomorphic to a subgroup of the symmetric group of degree 3. Therefore $|R : K| \leq 3! = 6$. Since by hypothesis A is not normal in R, we deduce that K is a proper subgroup of A. As $|R : A| = 3$ and $|R : K| \leq 6$, we get that $|R : K| = 6$ and that R/K is isomorphic to the dihedral group of order 6.

Suppose that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ky = \emptyset$, for some $y \in R \setminus A$. As $R \setminus A$ is the union of four K-cosets and as $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ky = \emptyset$, we deduce $|\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap (R \setminus A)| \leq 3|K|$. As $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A = \mathbf{I}(A)$, we get $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = |\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap (R \setminus A)| \leq |\mathbf{I}(A)| + 3|K|$ and hence

$$\begin{aligned} o &\leq \frac{1}{4}\left(\frac{4}{3}|R| + |\mathbf{I}(R)| + |\mathbf{I}(A)| + 3|K|\right) \leq \frac{1}{4}\left(\frac{4}{3}|R| + 2|\mathbf{I}(R)| + 3\frac{|R|}{6}\right) \\ &= \frac{1}{4}\left(\frac{11}{6}|R| + 2|\mathbf{I}(R)|\right) = \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{24} = \mathbf{c}(R) - \frac{|R|}{24}, \end{aligned}$$

and (1) holds in this case. Thus we may suppose $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Ky \neq \emptyset$, for every $y \in R \setminus A$.

Let $x_1, x_2, x_3, x_4 \in R \setminus A$ with $R = A \cup Kx_1 \cup Kx_2 \cup Kx_3 \cup Kx_4$ and with $x_1, x_2, x_3, x_4 \in \mathbf{C}_R(\varphi)^{\mathrm{inv}}$. As usual we denote by $\iota_{x_i} : K \to K$ the automorphism of K defined by $k^{\iota_{x_i}} = x_i k x_i^{-1}$, for every $k \in K$. For each $i \in \{1, \ldots, 4\}$, let $y \in \mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap Kx_i$. Then $y = kx_i$, for some $k \in K$ and hence $x_i^{-1}k^{-1} = (kx_i)^{-1} = y^{-1} = y^{\varphi} = (kx_i)^{\varphi} = k^{\varphi}x_i^{\varphi} = kx_i^{-1}$, that is, $x_i k x_i^{-1} = k^{-1}$ and $k \in \mathbf{C}_K(\iota_{x_i})^{\mathrm{inv}}$. This shows

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(A) \cup \mathbf{C}_K(\iota_{x_1})^{\mathrm{inv}}x_1 \cup \mathbf{C}_K(\iota_{x_2})^{\mathrm{inv}}x_2 \cup \mathbf{C}_K(\iota_{x_3})^{\mathrm{inv}}x_3 \cup \mathbf{C}_K(\iota_{x_4})^{\mathrm{inv}}x_4. \tag{2.5}$$

Suppose that $|\mathbf{C}_K(\iota_{x_i})^{\mathrm{inv}}| \leq 3|K|/4$, for some $i \in \{1, 2, 3, 4\}$. Then

$$|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq |\mathbf{I}(A)| + 3|K| + \frac{3|K|}{4} = |\mathbf{I}(A)| + \frac{15|K|}{4} = |\mathbf{I}(A)| + \frac{5|R|}{8}.$$

Thus

$$\begin{aligned} o &\leq \frac{1}{4}\left(\frac{4}{3}|R| + |\mathbf{I}(R)| + |\mathbf{I}(A)| + \frac{5|R|}{8}\right) \leq \frac{1}{4}\left(\frac{47}{24}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{96} = \mathbf{c}(R) - \frac{|R|}{96}, \end{aligned}$$

and (1) holds in this case. Therefore, we may suppose that $|\mathbf{C}_K(\iota_{x_i})^{\mathrm{inv}}| > 3|K|/4$, for each $i \in \{1,2,3,4\}$. The work of Miller [11] shows that K is abelian and that, for every $i \in \{1,2,3,4\}$, x_i acts by conjugation on K by inverting each of its elements. In particular, (2.5) becomes

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{I}(A) \cup (R \setminus A). \tag{2.6}$$

As R/K is isomorphic to the dihedral group of order 6, we deduce that there exist $i,j,k \in \{1,2,3,4\}$ with $x_i x_j \in K x_k$. From the previous paragraph, x_i, x_j and x_k act by conjugation on K by inverting each of its elements. Therefore, for every $y \in K$, we have

$$y^{-1} = y^{x_k} = y^{x_i x_j} = (y^{x_i})^{x_j} = (y^{-1})^{x_j} = y,$$

that is, $y^2 = 1$. This yields that K is an elementary abelian 2-group and hence $K \subseteq \mathbf{I}(A)$. Eq (2.6) gives $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \supseteq K \cup (R \setminus A)$ and hence $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \geq |K| + |R \setminus A| = 5|R|/6 > 3|R|/4$. Again, from the work of Miller [11], we deduce that R is abelian and $\varphi = \iota$, and (2) holds in this case. □

Before proving the main step towards the proof of Theorem 1.3, we need a preliminary observation.

Lemma 2.7. *Let φ be an automorphism of a finite group R and let*

$$\kappa := \frac{|\mathbf{C}_R(\varphi)^{inv}|}{|R|}.$$

If $\frac{1}{2} < \kappa < 1$, then there exists a positive integer $q \geq 2$ with $\kappa = \frac{q+1}{2q}$. In particular, if $\frac{2}{3} < \kappa$, then $\kappa = \frac{3}{4}$ and there exists an abelian subgroup A of R such that $|R : A| = |A : \mathbf{C}_A(x)| = 2$ for every $x \in R \setminus A$.

Proof. The first assertion follows at once from the classification of Liebeck and MacHale [10, Structure Theorem, page 61] of the finite groups admitting an automorphism inverting more than half of the elements. (Actually, the first statement of this lemma can also be found in the third paragraph of the introductory section in [10].)

Suppose now that $\frac{2}{3} < \kappa$. Then, from the first statement, there exists $q \in \mathbb{N}$ with $q \geq 2$ and $\kappa = \frac{q+1}{2q}$. Now, $\frac{2}{3} < \frac{q+1}{2q}$ only when $q = 2$; hence $\kappa = \frac{3}{4}$. We now invoke once again the work of Liebeck and MacHale. In [10, Structure Theorem, page 61], the finite groups admitting an automorphism inverting more than half of the elements are partitioned into three types. Namely, **Type I***, **Type II*** and **Type III***. It is readily seen that none of the groups in **Type II*** or **Type III*** admits an automorphism φ with $\frac{|\mathbf{C}_R(\varphi)^{\mathrm{inv}}|}{|R|} = \frac{3}{4}$. Therefore, R is of **Type I***, which means that there exists an abelian subgroup A with $|R : A| = |A : \mathbf{C}_A(x)|$, for every $x \in R \setminus A$. □

Lemma 2.8. *Let R be a finite group and let φ be a non-identity automorphism of R. Then, one of the following holds*

1. *the number of φ-invariant inverse-closed subsets of R is at most $2^{\mathbf{c}(R)-\frac{|R|}{96}}$,*
2. *$\mathbf{C}_R(\varphi)$ is abelian of exponent greater than 2 and has index 2 in R, R is a generalized dicyclic group over $\mathbf{C}_R(\varphi)$ and $\varphi = \bar{\iota}_{\mathbf{C}_R(\varphi)}$,*
3. *R is abelian of exponent greater than 2 and $\varphi = \iota$.*

Proof. In the first part of the proof, we establish the result when φ has order p, where p is a prime number.

Recall that $\iota : R \to R$ is the permutation of R defined by $x^\iota = x^{-1}$, for every $x \in R$. Let $H := \langle \iota, \varphi \rangle \leq \mathrm{Sym}(R)$. Clearly, the number of φ-invariant inverse-closed subsets of R is 2^o, where o is the number of H-orbits, that is, o is the number of orbits of H in its action on R. From the orbit-counting lemma, we have

$$o = \frac{1}{|H|} \sum_{h \in H} |\mathrm{Fix}_R(h)|, \tag{2.7}$$

where $\mathrm{Fix}_R(h) := \{x \in R \mid x^h = x\}$ is the fixed-point set of h in its action on R.

For every $x \in R$, we have $x^{\iota\varphi} = (x^{-1})^\varphi = (x^\varphi)^{-1} = x^{\varphi\iota}$ and hence $\iota\varphi = \varphi\iota$. Therefore H is an abelian group. Moreover, $\mathrm{Fix}_R(\iota) = \mathbf{I}(R)$ and $\mathrm{Fix}_R(\varphi^\ell) = \mathbf{C}_R(\varphi)$ for every $\ell \in \{1, \ldots, p-1\}$.

Suppose R is abelian of exponent at most 2. As R has exponent at most 2, ι is the identity permutation and hence $H = \langle \varphi \rangle$ is cyclic of prime order p. From (2.7) and from the fact that $|\mathbf{C}_R(\varphi)| \leq |R|/2$, we obtain

$$o = \frac{1}{p}(|R| + (p-1)|\mathbf{C}_R(\varphi)|) \leq \frac{1}{p}\left(|R| + (p-1)\frac{|R|}{2}\right) = \frac{(p+1)|R|}{2p} \leq \frac{3|R|}{4} = |R| - \frac{|R|}{4}$$

and part (1) of the lemma holds in this case because $\mathbf{c}(R) = (|R| + |\mathbf{I}(R)|)/2 = |R|$ and thus

$$o = |R| - \frac{|R|}{4} = \mathbf{c}(R) - \frac{|R|}{4}.$$

In particular, for the rest of the argument we suppose that R has exponent greater than 2. Thus H has order $2p$.

CASE 1: p is odd.

As H is abelian of order $2p$, we deduce that H is cyclic and $\mathrm{Fix}_R(\iota\varphi^\ell) = \mathbf{C}_R(\varphi^\ell) \cap \mathrm{Fix}_R(\iota) = \mathbf{C}_R(\varphi) \cap \mathbf{I}(R)$, for every $\ell \in \{1, \ldots, p-1\}$. Now, (2.7) yields (in the second inequality we are using the fact that φ is not the identity automorphism and hence $|\mathbf{C}_R(\varphi)| \leq |R|/2$)

$$\begin{aligned}
o &= \frac{1}{2p}\left(|R| + |\mathbf{I}(R)| + (p-1)|\mathbf{C}_R(\varphi)| + (p-1)|\mathbf{C}_R(\varphi) \cap \mathbf{I}(R)|\right) \\
&\leq \frac{1}{2p}\left(|R| + |\mathbf{I}(R)| + (p-1)|\mathbf{C}_R(\varphi)| + (p-1)|\mathbf{I}(R)|\right) \\
&= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{2} + \frac{1}{2p}\left(|R| + (p-1)|\mathbf{C}_R(\varphi)|\right) \\
&\leq \mathbf{c}(R) - \frac{|R|}{2} + \frac{1}{2p}\left(|R| + (p-1)\frac{|R|}{2}\right) = \mathbf{c}(R) - |R|\left(\frac{1}{2} - \frac{p+1}{4p}\right) \\
&= \mathbf{c}(R) - |R|\frac{p-1}{4p} \leq \mathbf{c}(R) - \frac{|R|}{6}.
\end{aligned}$$

CASE 2: $p = 2$.

If $\varphi = \iota$, then R is an abelian group of exponent greater than 2 and we obtain that part (3) holds in this case. Therefore, we may suppose that $\varphi \neq \iota$. As $H = \langle \varphi, \iota \rangle$ is abelian of order $2p$, we deduce that $H = \{id_R, \iota, \varphi, \iota\varphi\}$ is elementary abelian of order 4. Moreover, $\mathrm{Fix}_R(\iota) = \mathbf{I}(R)$, $\mathrm{Fix}_R(\varphi) = \mathbf{C}_R(\varphi)$ and $\mathrm{Fix}_R(\iota\varphi) := \mathbf{C}_R(\varphi)^{\mathrm{inv}}$. Thus

$$o = \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|\right).$$

From Lemmas 2.5 and 2.6, we may suppose that $|R : \mathbf{C}_R(\varphi)| \geq 4$.

Miller [11] has shown that a non-identity automorphism of a non-abelian group inverts at most $3|R|/4$ elements. Therefore, $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq 3|R|/4$. Observe that the same inequality holds when R is abelian because $\mathbf{C}_R(\varphi)^{\mathrm{inv}}$ is a proper subgroup of R and hence $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq |R|/2 \leq 3|R|/4$. In particular, if $|R : \mathbf{C}_R(\varphi)| \geq 5$, then we deduce

$$\begin{aligned} o &= \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + \frac{|R|}{5} + \frac{3|R|}{4}\right) \\ &= \frac{1}{4}\left(\frac{39}{20}|R| + |\mathbf{I}(R)|\right) \\ &\leq \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{80} = \mathbf{c}(R) - \frac{|R|}{80}. \end{aligned}$$

For the rest of the argument we may suppose that $|R : \mathbf{C}_R(\varphi)| \leq 4$ and hence $|R : \mathbf{C}_R(\varphi)| = 4$. Therefore

$$o = \frac{1}{4}\left(\frac{5|R|}{4} + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|\right). \tag{2.8}$$

Assume $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq 2|R|/3$. Then, from (2.8), we get

$$\begin{aligned} o &= \frac{1}{4}\left(\frac{5|R|}{4} + |\mathbf{I}(R)| + \frac{2|R|}{3}\right) \\ &= \frac{1}{4}\left(\frac{23}{12}|R| + |\mathbf{I}(R)|\right) \leq \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{48} = \mathbf{c}(R) - \frac{|R|}{48}. \end{aligned}$$

Therefore, we may assume that $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| > 2|R|/3$.

As $2|R|/3 < |\mathbf{C}_R(\varphi)^{\mathrm{inv}}| \leq 3|R|/4$, from Lemma 2.7 we deduce that

$$|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = \frac{3|R|}{4}$$

and that R contains an abelian subgroup A with $|R : A| = |A : \mathbf{C}_A(x)| = 2$, for every $x \in R \setminus A$.

Suppose that A is not φ-invariant. Since φ has order $p = 2$, $A \cap A^\varphi$ has index 4 in R and is φ-invariant. Observe that $R/(A \cap A^\varphi)$ is an elementary abelian 2-group of order 4. Let T be the index 2 subgroup of R containing $A \cap A^\varphi$ and with $A \neq T \neq A^\varphi$. We have

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A) \cup (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A^\varphi) \cup (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap T).$$

Let $a \in \mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A$. Then $a^{-1} = a^\varphi \in A^\varphi \cap A$ and hence $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A = \mathbf{C}_{A\cap A^\varphi}(\varphi)^{\mathrm{inv}}$ and (similarly) $\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A^\varphi = \mathbf{C}_{A\cap A^\varphi}(\varphi)^{\mathrm{inv}}$. Therefore

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{C}_{A\cap A^\varphi}(\varphi)^{\mathrm{inv}} \cup (\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap T).$$

We deduce

$$\begin{aligned} |\mathbf{C}_R(\varphi)^{\mathrm{inv}}| &= |\mathbf{C}_{A\cap A^\varphi}(\varphi)^{\mathrm{inv}}| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap (T \setminus (A \cap A^\varphi))| \\ &\le |A \cap A^\varphi| + (|T| - |A \cap A^\varphi|) \\ &= |T| = \frac{|R|}{2}; \end{aligned}$$

however this contradicts $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = 3|R|/4$. Thus A is φ-invariant.

CASE 2.1: φ inverts each element in A, that is, $a^\varphi = a^{-1}$, for every $a \in A$.

As $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = 3|R|/4 > |R|/2 = |A|$, there exists $x \in R \setminus A$ with $x^\varphi = x^{-1}$. It follows that $\mathbf{C}_R(\varphi)^{\mathrm{inv}} = A \cup \mathbf{C}_A(x)x$ and hence

$$|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = |A| + \frac{|A|}{2}. \tag{2.9}$$

A computation gives $\mathbf{C}_R(\varphi) = \mathbf{I}(A) \cup \{ax \mid a \in A, a^2 = x^{-2}\}$. Let $a, b \in A$ with the property that $a^2 = x^{-2} = b^2$. Then $(ab^{-1})^2 = a^2b^{-2} = x^{-2}x^2 = 1$. This shows that either $\{ax \mid a \in A, a^2 = x^{-2}\}$ is the empty set or $\{ax \mid a \in A, a^2 = x^{-2}\} = \{b\bar{a}x \mid b \in \mathbf{I}(A)\}$, where $\bar{a} \in A$ is a fixed element with $\bar{a}^2 = x^{-2}$. In particular, $|\mathbf{C}_R(\varphi)| \in \{|\mathbf{I}(A)|, 2|\mathbf{I}(A)|\}$. As $|R : \mathbf{C}_R(\varphi)| = 4$, we deduce that either $|A : \mathbf{I}(A)| = 2$ and $\{ax \mid a \in A, a^2 = x^{-2}\} = \emptyset$, or $|A : \mathbf{I}(A)| = 4$ and $\{ax \mid a \in A, a^2 = x^{-2}\} \neq \emptyset$. In the first case, from (2.9), we have

$$|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = |A| + |A|/2 = |A| + |\mathbf{I}(A)| \le \frac{|R|}{2} + |\mathbf{I}(R)|.$$

Thus

$$\begin{aligned} o &\le \frac{1}{4}\left(\frac{5}{4}|R| + |\mathbf{I}(R)| + \frac{|R|}{2} + |\mathbf{I}(R)|\right) \le \frac{1}{4}\left(\frac{7}{4}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{16} = \mathbf{c}(R) - \frac{|R|}{16}. \end{aligned}$$

In the second case, from (2.9), we have

$$\begin{aligned} |\mathbf{C}_R(\varphi)^{\mathrm{inv}}| &= |A| + |A|/2 = |A| + 2|\mathbf{I}(A)| \\ &= \frac{|R|}{2} + |\mathbf{I}(A)| + |\mathbf{I}(A)| = \frac{|R|}{2} + \frac{|R|}{8} + |\mathbf{I}(A)| \\ &\le \frac{5|R|}{8} + |\mathbf{I}(R)|. \end{aligned}$$

Thus

$$\begin{aligned} o &\le \frac{1}{4}\left(\frac{5}{4}|R| + |\mathbf{I}(R)| + \frac{5|R|}{8} + |\mathbf{I}(R)|\right) = \frac{1}{4}\left(\frac{15}{8}|R| + 2|\mathbf{I}(R)|\right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{32} = \mathbf{c}(R) - \frac{|R|}{32}. \end{aligned}$$

CASE 2.2: φ does not invert each element in $R \setminus A$.

Observe that $\mathbf{C}_A(\varphi)^{\mathrm{inv}}$ is a subgroup of A because A is abelian. In particular, $|\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A| \leq |A|/2 = |R|/4$. As $|\mathbf{C}_R(\varphi)^{\mathrm{inv}}| = 3|R|/4$, we deduce that

- φ inverts each element in $R \setminus A$ and
- $|\mathbf{C}_R(\varphi)^{\mathrm{inv}} \cap A| = |R|/4$.

Fix $x \in R \setminus A$. In particular, for every $a \in A$, we have $x^{-1}a^{-1} = (ax)^{-1} = (ax)^\varphi = a^\varphi x^\varphi = a^\varphi x^{-1}$ and hence $a^\varphi = x^{-1}a^{-1}x$. From this it follows

$$\mathbf{C}_R(\varphi)^{\mathrm{inv}} = \mathbf{C}_A(x) \cup Ax \text{ and } \mathbf{C}_R(\varphi) = \mathbf{C}_A(\iota_x)^{\mathrm{inv}} \cup \mathbf{I}(R \setminus A),$$

where $\mathbf{I}(R \setminus A) := \{m \in R \setminus A \mid m^2 = 1\}$.

Suppose that $\mathbf{I}(R \setminus A) = \emptyset$. Then $\mathbf{C}_R(\varphi) = \mathbf{C}_A(\iota_x)^{\mathrm{inv}}$ and hence $|A : \mathbf{C}_A(\iota_x)^{\mathrm{inv}}| = 2$ because $|R : \mathbf{C}_R(\varphi)| = 4$. As $|A : \mathbf{C}_A(x)| = 2$, we deduce that $|A : \mathbf{C}_A(x) \cap \mathbf{C}_A(\iota_x)^{\mathrm{inv}}| \leq 4$. Clearly, $\mathbf{C}_A(x) \cap \mathbf{C}_A(\iota_x)^{\mathrm{inv}} \subseteq \mathbf{I}(A)$ and hence $|A : \mathbf{I}(A)| \leq 4$. We deduce

$$\begin{aligned}|\mathbf{C}_R(\varphi)| = |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| &= |\mathbf{C}_A(\iota_x)^{\mathrm{inv}} \cap (A \setminus \mathbf{C}_A(x))| + |\mathbf{C}_A(\iota_x)^{\mathrm{inv}} \cap \mathbf{C}_A(x)| \\ &\leq \frac{|A|}{4} + |\mathbf{I}(A)| \leq \frac{|R|}{8} + |\mathbf{I}(R)|.\end{aligned}$$

Thus

$$\begin{aligned} o &= \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|\right) \\ &= \frac{1}{4}\left(\frac{7|R|}{4} + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)|\right) \leq \frac{1}{4}\left(\frac{7|R|}{4} + |\mathbf{I}(R)| + \frac{|R|}{8} + |\mathbf{I}(R)|\right) \\ &= \frac{1}{4}\left(\frac{15|R|}{8} + 2|\mathbf{I}(R)|\right) \leq \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{32} = \mathbf{c}(R) - \frac{|R|}{32}.\end{aligned}$$

Suppose that $\mathbf{I}(R \setminus A) \neq \emptyset$. In particular, we may suppose that $x \in \mathbf{I}(R \setminus A)$, that is, $x^2 = 1$. From this it follows that

$$\begin{aligned}\mathbf{C}_R(\varphi) &= \mathbf{C}_A(\iota_x)^{\mathrm{inv}} \cup \mathbf{C}_A(\iota_x)^{\mathrm{inv}}x, \\ \mathbf{C}_R(\varphi)^{\mathrm{inv}} &= \mathbf{C}_A(x) \cup Ax, \\ \mathbf{I}(R) &= \mathbf{I}(A) \cup \mathbf{C}_A(\iota_x)^{\mathrm{inv}}x.\end{aligned}$$

As $|\mathbf{C}_R(\varphi)| = |R|/4$, we deduce $|\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| = |A|/4$. Assume that $|\mathbf{I}(R)| \geq |\mathbf{C}_R(\varphi)|$, that is, $|\mathbf{I}(A)| \geq |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}|$. Thus

$$\begin{aligned} o &= \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + |\mathbf{C}_R(\varphi)| + |\mathbf{C}_R(\varphi)^{\mathrm{inv}}|\right) \\ &= \frac{1}{4}\left(\frac{7|R|}{4} + 2|\mathbf{I}(R)|\right) \leq \frac{|R| + |\mathbf{I}(R)|}{2} - \frac{|R|}{16} = \mathbf{c}(R) - \frac{|R|}{16}.\end{aligned}$$

Assume that $|\mathbf{I}(R)| < |\mathbf{C}_R(\varphi)|$, that is, $|\mathbf{I}(A)| < |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}|$. Observe now

$$\mathbf{C}_A(x) \cap \mathbf{I}(A) = \mathbf{C}_A(\iota_x)^{\mathrm{inv}} \cap \mathbf{I}(A) = \mathbf{C}_A(x) \cap \mathbf{C}_A(\iota_x)^{\mathrm{inv}}.$$

As $|\mathbf{I}(R)| < |\mathbf{C}_R(\varphi)|$, from these equalities we deduce $\mathbf{I}(A) = \mathbf{C}_A(x) \cap \mathbf{C}_A(\iota_x)^{\mathrm{inv}}$ and that $\mathbf{C}_A(x) \neq \mathbf{C}_A(\iota_x)^{\mathrm{inv}}$. Moreover,

$$|\mathbf{I}(A)| = \frac{|A|}{8},\ |\mathbf{C}_A(x)| = \frac{|A|}{2},\ |\mathbf{C}_A(\iota_x)^{\mathrm{inv}}| = \frac{|A|}{4}.$$

In particular, $\mathbf{c}(R) = (|R| + |\mathbf{I}(R)|)/2 = 19|R|/32$. Thus

$$o \;=\; \frac{1}{4}|R|\left(1 + \frac{3}{16} + \frac{1}{4} + \frac{3}{4}\right) = \frac{35|R|}{64} = \frac{19|R|}{32} - \frac{3|R|}{64} = \mathbf{c}(R) - \frac{3|R|}{64}.$$

The proof of the lemma is now completed when φ has prime order.

Suppose now that $o(\varphi)$ is not a prime number. Let p be the largest prime divisor of $o(\varphi)$ and let $\psi := \varphi^{o(\varphi)/p}$. As ψ is a non-identity automorphism of R of prime order, we are in the position to apply Lemma 2.8 to the group R and to the automorphism ψ. Let 2^o be the number of orbits of $\langle\varphi\rangle$ on R.

If part (1) of Lemma 2.8 holds for ψ, then part (1) of Lemma 2.8 holds for φ because every φ-invariant subset of R is also ψ-invariant.

Assume then that part (3) of Lemma 2.8 holds for ψ. Then R is abelian of exponent greater than 2 and $\psi = \iota$. Hence $p = o(\psi) = 2$. As p is the largest prime divisor of d, we deduce that d is a power of 2. As $o(\varphi) \geq 4$ and $\varphi^{d/2} = \iota$, the action of $\langle\varphi\rangle$ on R has orbits of cardinality 1 on $\mathbf{C}_R(\varphi)$, of cardinality at least 2 on $\mathbf{C}_R(\iota) \setminus \mathbf{C}_R(\varphi)$, and of cardinality at least 4 on $R \setminus \mathbf{C}_R(\iota)$. It follows that the number of subsets of R which are φ-invariant is at most

$$2^{|\mathbf{C}_R(\varphi)|} \cdot 2^{\frac{|\mathbf{C}_R(\iota)\setminus\mathbf{C}_R(\varphi)|}{2}} \cdot 2^{\frac{|R\setminus\mathbf{C}_R(\iota)|}{4}} = 2^{\frac{|R|+|\mathbf{C}_R(\iota)|}{4} + \frac{|\mathbf{C}_R(\varphi)|}{2}}.$$

Observe that every φ-invariant subset of R is also inverse-closed because $\varphi^{d/2} = \iota$. Thus

$$2^o \leq 2^{\frac{|R|+|\mathbf{C}_R(\iota)|}{4} + \frac{|\mathbf{C}_R(\varphi)|}{2}}.$$

Observe, also, that $\mathbf{C}_R(\iota) = \mathbf{I}(R)$. As $\mathbf{c}(R) = (|R| + |\mathbf{I}(R)|)/2$, by rewriting the previous equation, we deduce

$$2^o \leq 2^{\mathbf{c}(R) - \frac{|R|+|\mathbf{I}(R)|-2|\mathbf{C}_R(\varphi)|}{4}}. \tag{2.10}$$

If $|\mathbf{I}(R)| - 2|\mathbf{C}_R(\varphi)| \geq 0$, then (2.10) yields

$$o \leq 2^{\mathbf{c}(R) - \frac{|R|}{4}}.$$

Thus part (1) holds for R and φ. If $|\mathbf{I}(R)| - 2|\mathbf{C}_R(\varphi)| < 0$, then $|\mathbf{I}(R)| < 2|\mathbf{C}_R(\varphi)|$. However, as $\mathbf{C}_R(\varphi) \leq \mathbf{C}_R(\psi) = \mathbf{I}(R)$, we deduce $\mathbf{I}(R) = \mathbf{C}_R(\varphi)$ and hence (2.10) yields

$$o \leq 2^{\mathbf{c}(R) - \frac{|R|-|\mathbf{I}(R)|}{4}}.$$

Since R has exponent greater than 2, we have $|R| - |\mathbf{I}(R)| \leq |R|/2$ and hence

$$o \leq 2^{\mathbf{c}(R) - \frac{|R|}{8}}.$$

Thus part (1) holds for R and φ.

Assume then that part (2) of Lemma 2.8 holds for ψ. Then $\mathbf{C}_R(\psi)$ is abelian of exponent greater than 2 and has index 2 in R, R is a generalized dicyclic group over $\mathbf{C}_R(\psi)$

and $\psi = \bar{\iota}_{\mathbf{C}_R(\psi)}$. Hence $p = o(\psi) = 2$. As p is the largest prime divisor of d, we deduce that d is a power of 2. As $o(\varphi) \geq 4$ and $\varphi^{d/2} = \psi = \bar{\iota}_{\mathbf{C}_R(\psi)}$, the action of $\langle\varphi\rangle$ on R has orbits of cardinality 1 on $\mathbf{C}_R(\varphi)$, of cardinality at least 2 on $\mathbf{C}_R(\bar{\iota}_{\mathbf{C}_R(\psi)}) \setminus \mathbf{C}_R(\varphi)$, and of cardinality at least 4 on $R \setminus \mathbf{C}_R(\bar{\iota}_{\mathbf{C}_R(\psi)})$. As $\mathbf{C}_R(\psi) = \mathbf{C}_R(\bar{\iota}_{\mathbf{C}_R(\psi)})$, the action of $\langle\varphi\rangle$ on R has orbits of cardinality 1 on $\mathbf{C}_R(\varphi)$, of cardinality at least 2 on $\mathbf{C}_R(\psi) \setminus \mathbf{C}_R(\varphi)$, and of cardinality at least 4 on $R \setminus \mathbf{C}_R(\psi)$. Since the number of inverse-closed subsets of $\mathbf{C}_R(\varphi)$ is $\mathbf{c}(\mathbf{C}_R(\varphi)) = (|\mathbf{C}_R(\varphi)| + |\mathbf{I}(\mathbf{C}_R(\varphi))|)/2$, it follows that the number of inverse-closed subsets of R which are φ-invariant is at most

$$2^{\frac{|\mathbf{C}_R(\varphi)|+|\mathbf{I}(\mathbf{C}_R(\varphi))|}{2}} \cdot 2^{\frac{|\mathbf{C}_R(\psi)\setminus\mathbf{C}_R(\varphi)|}{2}} \cdot 2^{\frac{|R\setminus\mathbf{C}_R(\psi)|}{4}} = 2^{\frac{|R|+|\mathbf{C}_R(\psi)|}{4}+\frac{|\mathbf{I}(\mathbf{C}_R(\varphi))|}{2}}.$$

As $|\mathbf{C}_R(\psi)| = |R|/2$, we have

$$2^o \leq 2^{\frac{3|R|}{8}+\frac{|\mathbf{I}(\mathbf{C}_R(\varphi))|}{2}}.$$

As $\mathbf{c}(R) = (|R| + |\mathbf{I}(R)|)/2$, by rewriting the previous equation, we deduce

$$2^o \leq 2^{\mathbf{c}(R)-\frac{|R|+4|\mathbf{I}(R)|-4|\mathbf{I}(\mathbf{C}_R(\varphi))|}{8}}. \tag{2.11}$$

As $|\mathbf{I}(R)| - |\mathbf{I}(\mathbf{C}_R(\varphi))| \geq 0$, from (2.11) e deduce

$$2^o \leq 2^{\mathbf{c}(R)-\frac{|R|}{8}}.$$

In particular, part (1) holds for R and φ. □

Proposition 2.9. *Let R be a finite group and suppose that R is not an abelian group of exponent greater than 2 and that R is not a generalized dicyclic group. Then the set*

$$\{S \subseteq R \mid S = S^{-1}, R \neq \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\}$$

has cardinality at most $2^{\mathbf{c}(R)-|R|/96+(\log_2|R|)^2}$.

As $R \leq \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$, the condition $R \neq \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$ is equivalent to the fact that R is a proper subgroup of $\mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$.

Proof. Let, for the time being, R be any finite group. For every $\varphi \in \mathrm{Aut}(R)$ with $\varphi \neq id_R$ and for every $S \subseteq R$ with $S = S^{-1}$ and $S^\varphi = S$, we have $\varphi \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R) \setminus R$ and φ fixes the identity vertex of $\Gamma(R, S)$. Conversely, for every $S \subseteq R$ with $S = S^{-1}$ and for every $\varphi \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R) \setminus R$ with φ fixing the identity vertex of $\Gamma(R, S)$, we have $\varphi \in \mathrm{Aut}(R)$ with $\varphi \neq id_R$. Therefore,

$$\{S \subseteq R \mid S = S^{-1}, R \neq \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\} = \bigcup_{\substack{\varphi\in\mathrm{Aut}(R)\\ \varphi\neq id_R}} \{S \subseteq R \mid S = S^{-1}, S^\varphi = S\}$$

and

$$|\{S \subseteq R \mid S = S^{-1}, R \neq \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\}| = \sum_{\substack{\varphi\in\mathrm{Aut}(R)\\ \varphi\neq id_R}} |\{S \subseteq R \mid S = S^{-1}, S^\varphi = S\}|. \tag{2.12}$$

Suppose now that R is not an abelian group of exponent greater than 2 and that R is not a generalized dicyclic group.

Since a chain of subgroups of R has length at most $\log_2(|R|)$, R has a generating set of cardinality at most $\lfloor \log_2(|R|) \rfloor \leq \log_2(|R|)$. Any automorphism of R is uniquely determined by its action on the elements of a generating set for R. Therefore

$$|\operatorname{Aut}(R)| \leq |R|^{\lfloor \log_2(|R|) \rfloor} \leq 2^{(\log_2(|R|))^2}. \tag{2.13}$$

Let $\varphi \in \operatorname{Aut}(R)$ with $\varphi \neq id_R$. We now apply Lemma 2.8 to the group R and to the non-identity automorphism φ of R. As R is neither abelian of exponent greater than 2 nor generalized dicyclic, parts (2) and (3) of Lemma 2.8 do not hold. Hence, part (1) of Lemma 2.8 holds, that is,

$$|\{S \subseteq R \mid S = S^{-1}, S^{\varphi} = S\}| \leq 2^{\mathbf{c}(R) - \frac{|R|}{96}}. \tag{2.14}$$

Now the proof follows from (2.12), (2.13) and (2.14). □

3 Proofs of Theorems 1.3 and 1.6

Proof of Theorem 1.3. Let R be a finite group of order r which is neither generalized dicyclic nor abelian of exponent greater than 2. By Lemma 2.2 and Proposition 2.9, we have

$$\lim_{r\to\infty} \frac{|\{S \subseteq R \mid S = S^{-1}, R \neq \mathbf{N}_{\operatorname{Aut}(\Gamma(R,S))}(R)\}|}{|\{S \subseteq R \mid S = S^{-1}\}|} \leq \lim_{r\to\infty} 2^{-\frac{r}{96} + (\log_2(r))^2} = 0. \quad \square$$

Proof of Theorem 1.6. Let R be a finite group. It was shown in [3, 14] that Xu conjecture holds true when R is a generalized dicyclic group or when R is an abelian group of exponent greater than 2. In particular, for the rest of the proof we may assume that R is neither a generalized dicyclic group nor an abelian group of exponent greater than 2.

Let us denote by $\mathcal{N}(R) := \{S \subseteq R \mid S = S^{-1}, R \trianglelefteq \operatorname{Aut}(\Gamma(R,S))\}$, $\mathcal{C}(R) := \{S \subseteq R \mid S = S^{-1}, R = \operatorname{Aut}(\Gamma(R,S))\}$ and $\mathcal{T}(R) := \{S \subseteq R \mid S = S^{-1}\}$. If Conjecture 1.2 holds true, then

$$\lim_{|R|\to\infty} \frac{|\mathcal{C}(R)|}{|\mathcal{T}(R)|} = 1$$

and hence

$$\lim_{|R|\to\infty} \frac{|\mathcal{N}(R)|}{|\mathcal{T}(R)|} = 1,$$

because $\mathcal{C}(R) \subseteq \mathcal{N}(R)$, that is, Conjecture 1.5 holds true. Conversely, suppose that Conjecture 1.5 holds true, that is, $\lim_{|R|\to\infty} |\mathcal{N}(R)|/|\mathcal{T}(R)| = 1$. Now,

$$\begin{aligned} \mathcal{N}(R) &= \mathcal{C}(R) \cup \{S \subseteq R \mid S = S^{-1}, R \trianglelefteq \operatorname{Aut}(\Gamma(R,S)), R < \operatorname{Aut}(\Gamma(R,S))\} \\ &\subseteq \mathcal{C}(R) \cup \{S \subseteq R \mid S = S^{-1}, R < \mathbf{N}_{\operatorname{Aut}(\Gamma(R,S))}(R)\} \end{aligned}$$

and hence, by Theorem 1.3, we have

$$\begin{aligned} 1 &= \lim_{|R|\to\infty} \frac{|\mathcal{N}(R)|}{|\mathcal{T}(R)|} \\ &\leq \lim_{|R|\to\infty} \frac{|\mathcal{C}(R)|}{|\mathcal{T}(R)|} + \lim_{|R|\to\infty} \frac{|\{S \subseteq R \mid S = S^{-1}, R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\}|}{|\mathcal{T}(R)|} \\ &= \lim_{|R|\to\infty} \frac{|\mathcal{C}(R)|}{|\mathcal{T}(R)|}, \end{aligned}$$

that is, Theorem 1.2 holds true.

□

ORCID iDs

Pablo Spiga https://orcid.org/0000-0002-0157-7405

References

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

[2] L. Babai and C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15, doi:10.1016/s0195-6698(82)80003-6.

[3] E. Dobson, P. Spiga and G. Verret, Cayley graphs on abelian groups, *Combinatorica* **36** (2016), 371–393, doi:10.1007/s00493-015-3136-5.

[4] J. K. Doyle, T. W. Tucker and M. E. Watkins, Graphical Frobenius representations, *J. Algebraic Combin.* **48** (2018), 405–428, doi:10.1007/s10801-018-0814-6.

[5] C. D. Godsil, Grr's for non-solvable groups, in: *Algebraic Methods in Graph theory (Proc. Conf. Szeged 1978 L. Lovăsz and V. T. Sŏs, eds)*, North-Holland, Amsterdam, Coll. Math. Soc. J. Bolyai 25, pp. 221–239, 1981.

[6] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256, doi:10.1007/bf02579330.

[7] D. Hetzel, Über reguläre graphische darstellung von auflösbaren gruppen, Diploma thesis, Technische Universität, Berlin, 1976.

[8] W. Imrich, Graphical regular representations of groups of odd order, in: *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II*, North-Holland, Amsterdam-New York, volume 18 of *Colloq. Math. Soc. János Bolyai*, 1978 pp. 611–621.

[9] W. Imrich and M. E. Watkins, On graphical regular representations of cyclic extensions of groups, *Pacific J. Math.* **55** (1974), 461–477, http://projecteuclid.org/euclid.pjm/1102910980.

[10] H. Liebeck and D. MacHale, Groups with automorphisms inverting most elements, *Math. Z.* **124** (1972), 51–63, doi:10.1007/bf01142582.

[11] G. A. Miller, Groups Containing the Largest Possible Number of Operators of Order Two, *Amer. Math. Monthly* **12** (1905), 149–151, doi:10.2307/2969244.

[12] J. Morris, M. Moscatiello and P. Spiga, On the asymptotic enumeration of cayley graphs, 2018, arXiv:1811.07709 [math.CO].

[13] J. Morris, M. Moscatiello and P. Spiga, On the asymptotic enumeration of cayley graphs, 2020, arXiv:2005.07687 [math.CO].

[14] J. Morris, P. Spiga and G. Verret, Automorphisms of Cayley graphs on generalised dicyclic groups, *European J. Combin.* **43** (2015), 68–81, doi:10.1016/j.ejc.2014.07.003.

[15] L. A. Nowitz and M. E. Watkins, Graphical regular representations of non-abelian groups, i, *Canad. J. Math.* **24** (1972), 993–1008, doi:10.4153/cjm-1972-101-5.

[16] L. A. Nowitz and M. E. Watkins, Graphical regular representations of non-abelian groups, ii, *Canad. J. Math.* **24** (1972), 1009–1018, doi:10.4153/cjm-1972-102-3.

[17] P. Spiga, On the existence of Frobenius digraphical representations, *Electron. J. Combin.* **25** (2018), Paper No. 2.6, 19, doi:10.37236/7097.

[18] P. Spiga, On the existence of graphical frobenius representations and their asymptotic enumeration, *Journal Combin. Theory Series B* **142** (2020), 210–243, doi:10.1016/j.jctb.2019.10.003.

[19] M. E. Watkins, On the action of non-Abelian groups on graphs, *J. Combinatorial Theory Ser. B* **11** (1971), 95–104, doi:10.1016/0095-8956(71)90019-0.

[20] M. E. Watkins and L. A. Nowitz, On graphical regular representations of direct products of groups, *Monatsh. Math.* **76** (1972), 168–171, doi:10.1007/bf01298284.

[21] M.-Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, volume 182, 1998, doi:10.1016/s0012-365x(97)00152-0, graph theory (Lake Bled, 1995).