CC Creative Commons ADAM Logo

Also available at http://adam-journal.eu

The Art of Discrete and Applied Mathematics nn (year) 1–x

Groups for which it is easy to detect graphical regular representations

Dave Witte Morris , Joy Morris

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta. T1K 3M4, Canada

Gabriel Verret

Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

Received day month year, accepted xx xx xx, published online xx xx xx

Abstract

We say that a finite group G is *DRR-detecting* if, for every subset S of G, either the Cayley digraph $\mathrm{Cay}(G,S)$ is a digraphical regular representation (that is, its automorphism group acts regularly on its vertex set) or there is a nontrivial group automorphism φ of G such that $\varphi(S)=S$. We show that every nilpotent DRR-detecting group is a p-group, but that the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not DRR-detecting, for every odd prime p. We also show that if G_1 and G_2 are nontrivial groups that admit a digraphical regular representation and either $\gcd\big(|G_1|,|G_2|\big)=1$, or G_2 is not DRR-detecting, then the direct product $G_1 \times G_2$ is not DRR-detecting. Some of these results also have analogues for graphical regular representations.

Keywords: Cayley graph, GRR, DRR, automorphism group, normalizer

Math. Subj. Class.: 05C25,20B05

1 Introduction

All groups and graphs in this paper are finite. Recall [1] that a digraph Γ is said to be a *digraphical regular representation (DRR)* of a group G if the automorphism group of Γ is isomorphic to G and acts regularly on the vertex set of Γ. If a DRR of G happens to be a graph, then it is also called a *graphical regular representation (GRR)* of G. Other terminology and notation can be found in Section 2.

E-mail address: dave.morris@uleth.ca (Dave Witte Morris), joy.morris@uleth.ca (Joy Morris)g.verret@auckland.ac.nz (Gabriel Verret)

It is well known that if Γ is a GRR (or DRR) of G, then Γ must be a Cayley graph (or Cayley digraph, respectively), so there is a subset S of G such that $\Gamma \cong \operatorname{Cay}(G,S)$ (and S is inverse-closed if Γ is a graph). It is traditional [5, p. 243] to let

$$\operatorname{Aut}(G,S) = \{\, \varphi \in \operatorname{Aut}(G) \mid \varphi(S) = S \,\}.$$

Since $\operatorname{Aut}(G,S) \subseteq \operatorname{Aut}\bigl(\operatorname{Cay}(G,S)\bigr)$, it is obvious (and well known) that if $\operatorname{Aut}(G,S)$ is nontrivial, then $\operatorname{Cay}(G,S)$ is not a GRR (or DRR). In this paper, we discuss groups for which the converse holds:

Definition 1.1. We say that a group G is *GRR-detecting* if, for every inverse-closed subset S of G, $\operatorname{Aut}(G,S) = \{1\}$ implies that $\operatorname{Cay}(G,S)$ is a GRR. Similarly, a group G is *DRR-detecting* if for every subset S of G, $\operatorname{Aut}(G,S) = \{1\}$ implies that $\operatorname{Cay}(G,S)$ is a DRR.

Remark 1.2. Every Cayley graph is a Cayley digraph, so every DRR-detecting group is GRR-detecting.

Definition 1.3. We say that a Cayley (di)graph $\Gamma = \operatorname{Cay}(G,S)$ on a group G *witnesses that G is not GRR-detecting* (respectively, not DRR-detecting) if $\operatorname{Aut}(G,S) = \{1\}$ but Γ is not a GRR (respectively, not a DRR) for G.

An important class of DRR-detecting groups was found by Godsil. His result actually deals with vertex-transitive digraphs, rather than only the more restrictive class of Cayley graphs, but here is a special case of his result in our terminology:

Theorem 1.4 (Godsil, cf. [5, Corollary 3.9])**.** Let G be a p-group and let $\mathbb{Z}_p$ be the cyclic group of order p. If G admits no homomorphism onto the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ then G is DRR-detecting (and therefore also GRR-detecting).

Since $\mathbb{Z}_p \wr \mathbb{Z}_p$ is nonabelian, the following statement is an immediate consequence:

Corollary 1.5. Every abelian p-group is DRR-detecting (and therefore also GRR-detecting).

Remark 1.6. It is obvious (without reference to Theorem 1.4) that most abelian p-groups are GRR-detecting. Indeed, it is well known that every abelian group is GRR-detecting (unless it is an elementary abelian 2-group), because the nontrivial group automorphism $x \mapsto x^{-1}$ is an automorphism of $\operatorname{Cay}(G,S)$.

The following result shows that the bound in Godsil's theorem is sharp, in the sense that $\mathbb{Z}_p \wr \mathbb{Z}_p$ cannot be replaced with a larger p-group (when p is odd):

Theorem 1.7. If p is an odd prime, then the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not GRR-detecting (and is therefore also not DRR-detecting).

Remark 1.8. The conclusion of Theorem 1.7 is not true for $p = 2$, because $\mathbb{Z}_2 \wr \mathbb{Z}_2$ is GRR-detecting. This is a special case of the fact that if a group has no GRR, then it is GRR-detecting [4, Theorem 1.4].

The following two results provide additional examples, by showing that direct products often yield groups that are not DRR-detecting:

Theorem 1.9. If G_1 and G_2 are nontrivial groups that admit a DRR (a GRR, respectively) and $\gcd\bigl(|G_1|, |G_2|\bigr) = 1$, then $G_1 \times G_2$ is not DRR-detecting (not GRR-detecting, respectively).

Theorem 1.10. If G_1 admits a DRR (a GRR, respectively) and G_2 is not DRR-detecting (not GRR-detecting, respectively), then $G_1 \times G_2$ is not DRR-detecting (not GRR-detecting, respectively).

These two results are the main ingredients in the proof of the following theorem:

Theorem 1.11. Every nilpotent DRR-detecting group is a p-group.

Remark 1.12. The phrase "DRR-detecting" in Theorem 1.11 cannot be replaced with "GRR-detecting." For example, every abelian group is GRR-detecting (unless it is an elementary abelian 2-group), as was pointed out in Remark 1.6.

Here is an outline of the paper. A few definitions and basic results are recalled in Section 2. Theorem 1.7 is proved in Section 3. A generalization of Theorem 1.9 is proved in Section 4, by using wreath products of digraphs. In Section 5, we recall some fundamental facts about cartesian products of digraphs and use them to prove Theorem 1.10. Theorem 1.11 is proved in Section 6.

2 Preliminaries

Definition 2.1. Recall that if S is a subset of a group G, then the *Cayley digraph of G (with respect to the connection set S)* is the digraph $\mathrm{Cay}(G, S)$ whose vertex set is G, such that there is a directed edge from g_1 to g_2 if and only if $g_2 = sg_1$ for some $s \in S$. If S is closed under inverses, then $Cay(G, S)$ is a graph, and is called a *Cayley graph*.

See Remark 4.2 for a general definition of the wreath product of two groups. The following special case is less complicated:

Definition 2.2. Let $\mathbb{Z}_p \wr \mathbb{Z}_p = \mathbb{Z}_p \ltimes (\mathbb{Z}_p)^p$, where $\mathbb{Z}_p$ acts on $(\mathbb{Z}_p)^p$ by cyclically permuting the coordinates: for $(v_1, v_2, \ldots, v_p) \in (\mathbb{Z}_p)^p$ and $g \in \mathbb{Z}_p$, we have

$$(v_1, v_2, \ldots, v_p)^g = (v_{g+1}, v_{g+2}, \ldots, v_p, v_1, v_2, \ldots, v_g).$$

We will use the following well-known results.

Theorem 2.3 (Babai [1, Theorem 2.1])**.** If a finite group does not admit a DRR, then it is isomorphic to

$$Q_8,\ (\mathbb{Z}_2)^2,\ (\mathbb{Z}_2)^3,\ (\mathbb{Z}_2)^4, \text{ or } (\mathbb{Z}_3)^2,$$

where Q_8 is the quaternion group of order 8, which means

$$Q_8 = \langle\, i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k \,\rangle.$$

Lemma 2.4. Let $\widehat{G}$ be the right regular representation of G. Then:

1. $\widehat{G}$ is contained in $\mathrm{Aut}\big(\mathrm{Cay}(G, S)\big)$ for every subset S of G.
2. The normalizer of $\widehat{G}$ in $\mathrm{Aut}\big(\mathrm{Cay}(G, S)\big)$ is $\mathrm{Aut}(G, S) \ltimes \widehat{G}$.

The latter has the following simple consequence:

Lemma 2.5. If Γ is a Cayley digraph on G (a Cayley graph on G, respectively), then Γ witnesses that G is not DRR-detecting (not GRR-detecting, respectively) if and only if the regular representation of G is a proper self-normalizing subgroup of $\mathrm{Aut}(\Gamma)$.

3 $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not GRR-detecting

Let p be an odd prime. In this section, we show that $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not GRR-detecting. (This proves Theorem 1.7.) To do this, we will construct a Cayley graph Γ on $\mathbb{Z}_p \wr \mathbb{Z}_p$ such that Γ is not a GRR, but the regular representation of $\mathbb{Z}_p \wr \mathbb{Z}_p$ is self-normalizing in $\mathrm{Aut}(\Gamma)$. In order to construct this graph, we first construct a certain group G that properly contains $\mathbb{Z}_p \wr \mathbb{Z}_p$. We will then define Γ in such a way that G is contained in $\mathrm{Aut}(\Gamma)$.

Let $A \cong \mathbb{Z}_p$ be a cyclic group of order p, and choose an irreducible representation of A on a vector space $Q \cong (\mathbb{Z}_2)^n$ over the finite field with 2 elements, such that $n \geq 2$. Now construct the corresponding semidirect product $A \ltimes Q$, which is a nonabelian group of order $2^n p$.

Choose a nontrivial 1-dimensional representation $\chi \colon Q \to \{\pm 1\} \subseteq \mathbb{Z}_p^\times$ (where $\mathbb{Z}_p^\times$ denotes the multiplicative group of nonzero elements of $\mathbb{Z}_p$), and induce it to a representation of $A \ltimes Q$ on a vector space V over $\mathbb{Z}_p$ [10, §3.3, pp. 28–30]. Since Q has index p in $A \ltimes Q$, the vector space V has dimension p, so $V \cong (\mathbb{Z}_p)^p$. Let

$$G = (A \ltimes Q) \ltimes V.$$

Since the representation of $A \ltimes Q$ on V is induced from a one-dimensional representation of the normal subgroup Q, the restriction to Q decomposes as a direct sum of one-dimensional representations: $V = V_1 \oplus \cdots \oplus V_p$, where each V_i is a subgroup of order p that is normalized by Q (cf. [10, Proposition 22, p. 58]). (More precisely, for each $i \in \{1, \ldots, p\}$, there is some $a \in A$, such that the representation of Q on V_i is given by χ^a, where $\chi^a(g) = \chi(g^{a^{-1}})$ for $g \in Q$, and $g^h = h^{-1}gh$ for $g, h \in G$.) Note that, since A normalizes Q, it must (cyclically) permute the Q-irreducible summands $V_1, \ldots, V_p$, so the Sylow p-subgroup $A \ltimes V$ of G is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Fix a nonidentity element a of A. Since A normalizes Q, we know that the coset Qa is fixed by the action of Q on the space $Q\backslash G$ of right cosets of Q. Also fix some nonzero $v_1 \in V_1$. Then, for each $i \in \{1, \ldots, p\}$, let $v_i = v_1^{a^{i-1}}$, so v_i is a nonzero element of V_i, and define $z = v_1 + v_2 + \cdots + v_p$, so z is a generator of the center $\mathrm{Z}(A \ltimes V)$.

Now let

$$S = \big(\langle v_1, v_2 \rangle \smallsetminus \langle v_1 \rangle\big) \cup (a\, z^Q)^{\pm 1} \subseteq A \ltimes V \subseteq G,$$

and let

$$\Gamma = \mathrm{Cay}(A \ltimes V, S).$$

Since Q normalizes $\langle v_1 \rangle$ and $\langle v_2 \rangle$, and fixes the coset Qa in $Q\backslash G$, it is clear that $SQ = QS$. Therefore, after identifying the vertex set $A \ltimes V$ of Γ with $Q\backslash QAV = Q\backslash G$ in the natural way, we have $G \subseteq \mathrm{Aut}(\Gamma)$, via the natural action of G on $Q\backslash G$. (Note that the action of G on $Q\backslash G$ is faithful, because Q does not contain any nontrivial, normal subgroup of G. Otherwise, since the action of A on Q is irreducible, the entire subgroup Q would have to be normal, which would mean that Q acts trivially on $Q\backslash G$. But this is false, because the representation of Q on V is nontrivial.) So Γ is not a GRR.

Therefore, in order to show that $\mathbb{Z}_p \wr \mathbb{Z}_p \cong A \ltimes V$ is not GRR-detecting, it will suffice to show that $\mathrm{Aut}(A \ltimes V, S)$ is trivial. To this end, let φ be an automorphism of $A \ltimes V$ that fixes S. We will show that φ is trivial.

Since V is characteristic in $A \ltimes V$ (for example, it is the only abelian subgroup of order p^p), we know that

$$\varphi(V \cap S) = V \cap S = \langle v_1, v_2 \rangle \smallsetminus \langle v_1 \rangle \subseteq \langle v_1, v_2 \rangle.$$

So

$$\varphi\big(\langle v_1, v_2\rangle\big) = \varphi\big(\langle v_1 v_2, v_2\rangle\big) = \langle \varphi(v_1 v_2), \varphi(v_2)\rangle \subseteq \langle \varphi(V \cap S)\rangle \subseteq \langle v_1, v_2\rangle.$$

Since φ is injective, we conclude that φ fixes $\langle v_1, v_2\rangle$ (setwise). Then φ also fixes $\langle v_1, v_2\rangle \smallsetminus S = \langle v_1\rangle$.

We have $\varphi(a) \notin V$ (because $a \notin V$ and φ fixes V), which means $\varphi(a) = a^k v'$ for some $k \in \mathbb{Z}_p^\times$ and $v' \in V$. Then (since v' centralizes V, because V is abelian) we have

$$\langle v_1, v_2\rangle = \varphi\big(\langle v_1, v_2\rangle\big) \ni \varphi(v_2) = \varphi(v_1^a) = \varphi(v_1)^{\varphi(a)} \in \langle v_1\rangle^{a^k} = \langle v_{k+1}\rangle,$$

so $k \in \{0,1\} \cap \mathbb{Z}_p^\times = \{1\}$, which means

$$\varphi(a) = av'.$$

Note that (since $\varphi(V) = V$) this implies

$$\varphi(aV) = aV.$$

Since φ fixes $\langle v_1\rangle$, we have $\varphi(v_1) = \ell v_1$ for some $\ell \in \mathbb{Z}_p^\times$. For every $i \in \{1, \ldots, p\}$, this implies

$$\varphi(v_i) = \varphi(v_1^{a^{i-1}}) = \varphi(v_1)^{\varphi(a^{i-1})} = (\ell v_1)^{a^{i-1}} = \ell v_i.$$

Since $\{v_1, \ldots, v_p\}$ generates V, we conclude that

$$\varphi(v) = \ell v \text{ for all } v \in V.$$

To complete the proof, we will show that v' is trivial and $\ell = 1$. (This means that φ fixes a, and also fixes every element of V. So φ is the trivial automorphism, as desired.) For all $z_0 \in z^Q$, we have

$$\begin{aligned} a \cdot (v' + \ell z_0) &= a\, v' \cdot (\ell z_0) = \varphi(a)\, \varphi(z_0) = \varphi(a\, z_0) \\ &\in \varphi(S \cap aV) = \varphi(S) \cap \varphi(aV) = S \cap aV = a\, z^Q. \end{aligned}$$

Therefore, if we write $v' = \sum_{i=1}^p s_i v_i$ (with $s_i \in \mathbb{Z}_p$) and $z_0 = \sum_{i=1}^p t_i v_i$ (with $t_i \in \{\pm 1\}$), then we have

$$s_i + \ell t_i \in \{\pm 1\} \pmod p \text{ for every } i.$$

For any given i, the representation of Q on V_i is nontrivial, so we may choose z_0 so that $t_i = -1$. Therefore, we have $s_i - \ell \equiv \pm 1 \pmod p$. On the other hand, by letting $z_0 = z$ (and noting that $s_i - \ell \not\equiv s_i + \ell \pmod p$) we see that we also have $s_i + \ell \equiv \mp 1 \pmod p$. Adding these two equations and dividing by 2 yields $s_i = 0$ (for all i). So v' is trivial (which means $\varphi(a) = a$).

All that remains is to show that $\ell = 1$ (which means that φ acts trivially on V). Suppose this is not true. (That is, suppose $\ell \neq 1$.) We have

$$\pm \ell = 0 + \ell(\pm 1) = s_i + \ell t_i \in \{\pm 1\} \pmod p,$$

so this implies $\ell = -1$.

For convenience, let $Z = \langle z \rangle = \mathrm{Z}(A \ltimes V)$. Note that, since $\varphi(a) = a$, we have

$$a \cdot (-z) = a \cdot (\ell z) = \varphi(az) \in \varphi(S \cap aV) = S \cap aV = a\, z^Q,$$

so there is some $g \in Q$, such that $z^g = -z$. Since $Z = \langle z \rangle$, this implies that g is an element of the normaliser $\mathrm{N}_Q(Z)$ of Z in Q. Also note that g is nontrivial, because $z^g = -z \neq z$. Then, since $\mathrm{N}_Q(Z)$ is normalized by A (because A normalizes Q and Z), the irreducibility of the representation of A on Q implies that $\mathrm{N}_Q(Z) = Q$.

Hence, Q acts on Z by conjugation, so $Q/C_Q(Z)$ embeds in the cyclic group $\mathrm{Aut}(Z) \cong \mathbb{Z}_p^\times$. Since Q is an elementary abelian 2-group, this implies that $|Q/C_Q(Z)| \leq 2$. It is clear that $|Q| \geq 4$ (because $Q \cong (\mathbb{Z}_2)^n$ and $n \geq 2$), so we conclude that $C_Q(Z)$ is nontrivial. Using once again the fact that the representation of A on Q is irreducible, we conclude that $C_Q(Z) = Q$, which means that Q centralizes Z. However, since

$$Z = \langle z \rangle = \langle v_1 + v_2 + \cdots + v_p \rangle,$$

and each $\langle v_i \rangle = V_i$ is a Q-invariant subspace, this implies that Q centralizes each v_i, and is therefore trivial on V. On the other hand, we have $z^g = -z \neq z$, and $g \in Q$. This is a contradiction.

4 Using wreath products to construct witnesses

In this section, we prove Corollary 4.9, which is a generalization of Theorem 1.9.

Notation 4.1. In this section, N always denotes a normal subgroup of a group G. We let $\overline{G} = G/N$, and use $^-\colon G \to \overline{G}$ to denote the natural homomorphism.

Notation 4.2. For each $c \in G$ and each function $f\colon \overline{G} \to N$, we let $\varphi_{c,f}$ be the permutation on G that is defined by

$$\varphi_{c,f}(x) = xc\, f(\overline{x}) \text{ for } x \in G.$$

Let $W(G,N)$ be the set of all such permutations of G.

Remark 4.1. Informally speaking, an element of $W(G,N)$ is defined by choosing an element of $\overline{G}$ (or, more accurately, by choosing a coset representative) to permute the cosets of N, and then choosing an element of N to act on each coset. (The elements of N can be chosen independently on each coset.)

We have $\varphi_{c,f} = \varphi_{c',f'}$ if and only if there is some $n \in N$, such that $c' = cn$ and $f'(\overline{x}) = n^{-1} f(x)$ for all $\overline{x}$. From this, it follows that $|W(G,N)| = |\overline{G}| \cdot |N|^{|\overline{G}|}$.

Remark 4.2. The usual definition of the *wreath product* of two groups K and H is essentially:

$$K \wr H = W(K \times H, \{1\} \times H).$$

Definition 4.3. Recall that the *wreath product* $X \wr Y$ of two (di)graphs X and Y is the (di)graph whose vertex set is the cartesian product $V(X) \times V(Y)$, and with a (directed) edge from (x_1, y_1) to (x_2, y_2) if and only if either there is a (directed) edge from x_1 to x_2 or $x_1 = x_2$ and there is a (directed) edge from y_1 to y_2. This is also known as the *lexicographic product* of X and Y.

The following two observations are well known (and fairly immediate from the definitions). The first is a concrete version of the Universal Embedding Theorem, which states that G is isomorphic to a subgroup of $(G/N) \wr N$.

Lemma 4.4. $W(G,N)$ is a subgroup of the symmetric group on G. It is isomorphic to the wreath product $\overline{G} \wr N$, and contains the regular representation of G.

Lemma 4.5. Suppose $\mathrm{Cay}(\overline{G}, \overline{S_1})$ is a loopless Cayley digraph on $\overline{G}$, and $\mathrm{Cay}(N, S_2)$ is a Cayley digraph on N. Let $S_1 = \{\, g \in G \mid \overline{g} \in \overline{S_1} \,\}$. Then

$$\mathrm{Cay}(G, S_1 \cup S_2) \cong \mathrm{Cay}(\overline{G}, \overline{S_1}) \wr \mathrm{Cay}(N, S_2),$$

and $W(G,N)$ is contained in the automorphism group of $\mathrm{Cay}(G, S_1 \cup S_2)$.

The following result is a special case of the general principle that the automorphism group of a wreath product of digraphs is usually the wreath product of the automorphism groups. We have stated it only for DRRs, making use of some straightforward observations about the automorphism group of a DRR on more than 2 vertices, but the much more general statement in [3] applies to all vertex-transitive digraphs.

Lemma 4.6 (cf. Dobson-Morris [3, Theorem 5.7])**.** Assume that $\mathrm{Cay}(\overline{G}, \overline{S_1})$ and $\mathrm{Cay}(N, S_2)$ are loopless DRRs, and let S_1 be as in Lemma 4.5. If either $|\overline{G}| \neq 2$ or $|N| \neq 2$, then

$$\mathrm{Aut}\big(\mathrm{Cay}(G, S_1 \cup S_2)\big) = W(G,N).$$

In light of Lemmas 2.5 and 4.6, it is of obvious interest to us to determine when the regular representation of G is self-normalizing in $W(G,N)$. Our next result is the answer to this question. Recall that the *abelianization* of a group H is the largest abelian quotient of H, or, in other words, the quotient group $H/[H,H]$, where $[H,H]$ is the commutator subgroup of H.

Theorem 4.7. Let N be a normal subgroup of G. Then the regular representation of G is self-normalizing in $W(G,N)$ if and only if

1. $\mathrm{Z}(N) \leq \mathrm{Z}(G)$, and
2. the order of the abelianization of G/N is relatively prime to $|\mathrm{Z}(N)|$.

Proof. ($\Rightarrow$) We prove the contrapositive. (1) If $\mathrm{Z}(N) \not\leq \mathrm{Z}(G)$, then there exists $n \in \mathrm{Z}(N)$ such that $n \notin \mathrm{Z}(G)$. Conjugation by n is an element of $W(G,N)$ that normalizes the right regular representation of G, but is not in the right regular representation of G. (2) If the order of the abelianization of G/N is not relatively prime to $|\mathrm{Z}(N)|$, then there is a nontrivial homomorphism $f\colon \overline{G} \to \mathrm{Z}(N)$. We may assume that hypothesis (1) is satisfied, and then it is straightforward to verify that the corresponding element $\varphi_{f,1}$ of $W(G,N)$ normalizes the right regular representation of G:

$$\begin{aligned}
\varphi_{f,1}(xg) &= xg\, f(\overline{xg}) && \text{(definition of } \varphi_{f,1}\text{)}\\
&= x\, f(\overline{xg})\, g && (f(\overline{xg}) \in f(\overline{G}) \subseteq \mathrm{Z}(N) \subseteq \mathrm{Z}(G))\\
&= x\, f(\overline{x})\, f(\overline{g})\, g && (f \text{ is a homomorphism})\\
&= \varphi_{f,1}(x) \cdot f(\overline{g})\, g && \text{(definition of } \varphi_{f,1}\text{).}
\end{aligned}$$

($\Leftarrow$) By Lemma 2.4, it suffices to show that $\mathrm{Aut}(G) \cap W(G,N)$ is trivial. To this end, let $\varphi \in \mathrm{Aut}(G) \cap W(G,N)$. Since $\varphi \in W(G,N)$, there exist $c \in G$ and $f\colon \overline{G} \to N$, such that

$$\varphi(x) = xc\, f(\overline{x}) \text{ for all } x \in G.$$

Since φ is a group automorphism we know $\varphi(1) = 1 \in N$, so we may assume $c = 1$, after multiplying c on the right by an element of N. Then we must have $f(\overline{1}) = 1$. Now, for each $n \in N$, we have $\overline{n} = \overline{1}$, so

$$\varphi(n) = n \cdot f(\overline{n}) = n \cdot f(\overline{1}) = n \cdot 1 = n.$$

Therefore, for all $g \in G$ and $n \in N$, we have

$$gn \cdot f(\overline{g}) = gn \cdot f(\overline{gn}) = \varphi(gn) = \varphi(g)\,\varphi(n) = g\,f(\overline{g}) \cdot n,$$

so $n \cdot f(\overline{g}) = f(\overline{g}) \cdot n$. Since this is true for all $n \in N$, we conclude that $f(\overline{g}) \in \mathrm{Z}(N)$. Since $\mathrm{Z}(N) \subseteq \mathrm{Z}(G)$, this implies $f(\overline{g}) \in \mathrm{Z}(G)$ for all $\overline{g}$. Therefore, for all $g, h \in G$, we have

$$gh \cdot f(\overline{gh}) = \varphi(gh) = \varphi(g)\,\varphi(h) = g\,f(\overline{g}) \cdot h\,f(\overline{h}) = gh \cdot f(\overline{g})\,f(\overline{h}).$$

So f is a group homomorphism. Since $f(\overline{G})$ is contained in $\mathrm{Z}(N)$, which is abelian, we see from (2) that f must be trivial. Since c is also trivial, we conclude that $\varphi(x) = x$ for all x. Since φ is an arbitrary element of $\mathrm{Aut}(G) \cap W(G,N)$, this completes the proof. □

Remark 4.8. A slight modification of the proof of Theorem 4.7 shows that if $\widehat{G}$ is the right regular representation of G, then the normalizer of $\widehat{G}$ in $W(G,N)$ is

$$\{\, \varphi_{c,f} \mid c \in G, f \in Z^1\big(\overline{G}, \mathrm{Z}(N)\big) \,\},$$

where

$$Z^1\big(\overline{G}, \mathrm{Z}(N)\big) = \{\, f \colon \overline{G} \to \mathrm{Z}(N) \mid f(\overline{gh}) = f(\overline{g})^{\overline{h}}\, f(\overline{h}) \text{ for all } \overline{g}, \overline{h} \in \overline{G} \,\}$$

is the set of all "1-cocycles" or "crossed homomorphisms" from $\overline{G}$ to $\mathrm{Z}(N)$ (in the terminology of group cohomology [12]). This fact is presumably known.

It may also be of interest to note that hypotheses (1) and (2) in Theorem 4.7 are obviously satisfied when $\mathrm{Z}(N)$ is trivial.

Combining the results of this section, we obtain the following.

Corollary 4.9. Let N be a nontrivial, proper, normal subgroup of G, such that N and G/N each admit a DRR (or, respectively, a GRR). If

1. $\mathrm{Z}(N) \leq \mathrm{Z}(G)$, and
2. the order of the abelianization of G/N is relatively prime to $|\mathrm{Z}(N)|$,

then G is not DRR-detecting (respectively, not GRR-detecting).

More precisely, if we let Γ_1 be a DRR (respectively, GRR) on G/N and Γ_2 be a DRR (respectively, GRR) on N, then $\Gamma_1 \wr \Gamma_2$ witnesses that G is not DRR-detecting (respectively, not GRR-detecting).

Proof. Clearly, either $|\overline{G}| \neq 2$ or $|N| \neq 2$. It then follows by Lemma 4.5 and Lemma 4.6 that $\mathrm{Aut}\big(\Gamma_1 \wr \Gamma_2\big) = W(G,N)$. By Theorem 4.7, the regular representation of G is self-normalizing in $W(G,N)$, therefore $\Gamma_1 \wr \Gamma_2$ witnesses that G is not DRR-detecting (respectively, not GRR-detecting). □

Note that Theorem 1.9 can be obtained from Corollary 4.9 by letting $G = G_1 \times G_2$ and $N = G_2$.

5 Using cartesian products to construct witnesses

Definition 5.1. Recall that the *cartesian product* $X \mathbin{\square} Y$ of two (di)graphs X and Y is the (di)graph whose vertex set is the cartesian product $X \times Y$, such that there is a (directed) edge from (x_1, y_1) to (x_2, y_2) if and only if either $x_1 = x_2$ and there is a (directed) edge from y_1 to y_2, or $y_1 = y_2$, and there is a (directed) edge from x_1 to x_2.

We say that a (di)graph is *prime* (with respect to cartesian product) if it has more than one vertex, and is not isomorphic to the cartesian product of two (di)graphs, each with more than one vertex. It is well known that every (di)graph can be written uniquely as a cartesian product of prime factors (up to a permutation of the factors), but we do not need this fact.

To avoid the need to consider permutations of the factors, the following result includes the hypothesis that the factors are pairwise non-isomorphic. (This is not assumed in [11], which also considers isomorphisms between two different cartesian products, instead of only automorphisms of a single digraph.) The upshot is that, in this situation, the automorphism group of the cartesian product is the direct product of the automorphism groups.

Theorem 5.2 (Walker, cf. [11, Theorem 10])**.** Let $\Gamma_1, \ldots, \Gamma_k$ be weakly connected prime digraphs that are pairwise non-isomorphic. If φ is an automorphism of $\Gamma_1 \mathbin{\square} \cdots \mathbin{\square} \Gamma_k$, then for each i, there is an automorphism φ_i of Γ_i such that, for every vertex $(v_1, \ldots, v_k)$ of $\Gamma_1 \mathbin{\square} \cdots \mathbin{\square} \Gamma_k$, we have

$$\varphi(v_1, \ldots, v_k) = \big(\varphi_1(v_1), \ldots, \varphi_k(v_k)\big).$$

Prime graphs are quite abundant:

Theorem 5.3 (Imrich [7, Theorem 1])**.** If Γ is a graph (with more than one vertex), such that neither Γ nor its complement $\overline{\Gamma}$ is prime, then Γ is one of the following:

1. the cycle of length 4 or its complement (two disjoint copies of K_2);
2. the cube or its complement (the graph $K_2 \times K_4$);
3. $K_3 \mathbin{\square} K_3$ (which is self-complementary); or
4. $K_2 \mathbin{\square} \Delta$, where Δ is the graph obtained by deleting an edge from K_4 (which is self-complementary).

The following is an analogous result for digraphs. (Recall that a digraph is *proper* if it is not a graph.)

Theorem 5.4 (Grech-Imrich-Krystek-Wojakowski [6, Theorem 1.2] and Morgan-Morris-Verret [8, Theorem 2.2])**.** If Γ is a proper digraph, then at least one of Γ or $\overline{\Gamma}$ is prime.

Corollary 5.5. If a nontrivial group G admits a DRR (respectively, GRR), then it admits a DRR (respectively, GRR) that is prime (and weakly connected). Furthermore, if G is not DRR-detecting (respectively, not GRR-detecting), then there is a witness that is prime (and weakly connected).

Proof. First, note that Γ and $\overline{\Gamma}$ have the same automorphism group, so Γ is a DRR (GRR, respectively) for G if and only if $\overline{\Gamma}$ is. Similarly, Γ is a witness that G is not DRR-detecting (GRR-detecting, respectively) if and only if $\overline{\Gamma}$ is.

Also note that if a prime digraph Γ is not weakly connected, and is either a DRR or a witness that some group is not DRR-detecting, then $\overline{\Gamma} = K_2$ (so $\overline{\Gamma}$ is prime and weakly connected). This is because any vertex-transitive digraph is isomorphic to $\Gamma_0 \,\square\, \overline{K_n}$, where Γ_0 is a weakly connected component of the digraph, and n is the number of components.

Suppose that Γ is a GRR for G. By Theorem 5.3, at least one of Γ or $\overline{\Gamma}$ is prime with respect to cartesian product, unless Γ is one of the graphs listed in that theorem, but none of those graphs is a GRR, because the automorphism group does not act regularly on the set of vertices:

1. the automorphism group of a cycle of length 4 (or its complement) is the dihedral group of order 8;
2. the automorphism group of the cube (or its complement) is $\mathbb{Z}_2 \times \mathrm{Sym}(4)$, of order 48;
3. the automorphism group of $K_3 \,\square\, K_3$ is $\mathbb{Z}_2 \wr \mathrm{Sym}(3)$, of order 72; and
4. the graph $K_2 \,\square\, \Delta$ is not vertex-transitive (it is not even true that all vertices have the same valency).

Now, suppose that Γ is a DRR for G. We may assume that Γ is a proper digraph. (Otherwise, Γ is a GRR, so the preceding paragraph applies.) Then, by Theorem 5.4, either Γ or $\overline{\Gamma}$ is prime with respect to cartesian product.

Finally, suppose Γ is a witness that G is not DRR-detecting (or not GRR-detecting, respectively), such that neither Γ nor $\overline{\Gamma}$ is prime. This implies that Γ is one of the graphs listed in Theorem 5.3. (So G is not GRR-detecting.)

However, it is easy to see that none of the graphs listed in Theorem 5.3 is a witness. First, recall that a p-subgroup of a group cannot be self-normalizing unless it is a Sylow subgroup. Therefore (by Lemma 2.5), if a graph Γ of prime-power order p^k is a witness that some group is not GRR-detecting, then p^k must be the largest power of p that divides $\mathrm{Aut}(\Gamma)$. This shows that the graphs in (1) and (2) are not witnesses. If Γ is as described in (3), then the only regular subgroup of $\mathrm{Aut}(\Gamma)$ is the unique (Sylow) subgroup of order 9, which is normal, and is therefore obviously not self-normalizing. Finally, as noted above, the graphs in (4) are not vertex-transitive. □

Proof of Theorem 1.10. For simplicity, we consider only DRRs (because the proof is the same for GRRs). Let $\Gamma_1 = \mathrm{Cay}(G_1, S_1)$ be a DRR for G_1, and let $\Gamma_2 = \mathrm{Cay}(G_2, S_2)$ be a witness that G_2 is not DRR-detecting. By Corollary 5.5, we may assume that Γ_1 and Γ_2 are prime with respect to cartesian product (and are weakly connected). Since Γ_1 is a DRR, but Γ_2 is not, we know that $\Gamma_1 \not\cong \Gamma_2$. Therefore, we see from Theorem 5.2 that $\mathrm{Aut}(\Gamma_1 \,\square\, \Gamma_2) = \mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2)$.

Since Γ_2 is not a DRR, $\Gamma_1 \,\square\, \Gamma_2$ is not a DRR. Similarly, since the regular representation of G_1 is all of $\mathrm{Aut}(\Gamma_1)$ and the regular representation of G_2 is self-normalizing in $\mathrm{Aut}(\Gamma_2)$, the regular representation of $G_1 \times G_2$ is self-normalizing in $\mathrm{Aut}(\Gamma_1 \,\square\, \Gamma_2)$. So $\Gamma_1 \,\square\, \Gamma_2$ is a witness that $G_1 \times G_2$ is not DRR-detecting. □

6 Nilpotent DRR-detecting groups are p-groups

In this section, we prove Theorem 1.11, which states that if a nilpotent group is not a p-group, then it is not DRR-detecting. In most cases, this follows easily from Theorems 1.9 and 1.10, but there is one special case that requires a different proof:

Lemma 6.1. If H is a nontrivial group of odd order and $H \not\cong \mathbb{Z}_3 \times \mathbb{Z}_3$, then $Q_8 \times H$ is not DRR-detecting.

Proof. From Theorem 2.3, we see that H admits a DRR (because it has odd order, but is not $\mathbb{Z}_3 \times \mathbb{Z}_3$), so we may let $\mathrm{Cay}(H, S_1)$ be a DRR. Let $S = S_1 \cup \{i\} \cup jH \subseteq G$. It suffices to show that $\mathrm{Aut}(G, S) = \{1\}$ and that $\mathrm{Cay}(G, S)$ is not a DRR.

Let $\varphi \in \mathrm{Aut}(G, S)$. We can characterise S_1 as the set of all elements of S that have odd order. Thus, we must have $\varphi(S_1) = S_1$, so $H = \langle S_1 \rangle$ is fixed setwise by φ. Since the identity vertex is also fixed and the induced subgraph on H is a DRR, every element of H must be fixed by φ. We can use this fact to distinguish i from the elements of jH (all of which differ from each other by elements of H), so i is fixed by φ. Finally, j is the unique element of order 4 in jH, so it too is fixed by φ. We now know that φ is an automorphism of G that fixes every element of a generating set for G. So φ must be trivial.

All that remains is to show that $\mathrm{Cay}(G, S)$ is not a DRR. Fix a nontrivial element $h \in H$, and define a permutation τ of G by

$$\tau(x) = \begin{cases} x & \text{if } x \in \langle H, i \rangle; \\ xh & \text{if } x \in j\langle H, i \rangle. \end{cases}$$

Note that τ is a permutation of G, because right multiplication by h is a permutation of G that fixes $\langle H, i \rangle$ setwise.

We claim that τ is an automorphism of $\mathrm{Cay}(G, S)$. First, note that a directed edge of the form $g \to s_1 g$ or $g \to ig$ either has both of its endpoints in $\langle H, i \rangle$, or has both of its endpoints in $j\langle H, i \rangle$. Since right multiplication by h is an automorphism of $\mathrm{Cay}(G, S)$, it is clear that τ preserves such directed edges. The remaining directed edges are of the form $g \to gjh'$ for some $h' \in H$. Multiplying either g or gjh' on the right by h results in another such directed edge. This completes the proof that τ is an automorphism of $\mathrm{Cay}(G, S)$. □

Proof of Theorem 1.11. Let G be a nilpotent group, and assume that G is not a p-group. (Note that $|G|$ is divisible by at least two distinct primes.) We will show that G is not DRR-detecting.

Case 1. $|G|$ is divisible by at least three distinct primes. Let p be the largest prime divisor of $|G|$ and let P be a Sylow p-subgroup of G. Since G is nilpotent, we may write $G = P \times H$ for some subgroup H with $\gcd\big(|P|, |H|\big) = 1$. Since p is the largest of at least three primes dividing $|G|$, neither P nor H is a 2-group or a 3-group, so we see from Theorem 2.3 that P and H each admit a DRR. Therefore, Theorem 1.9 implies that $G = P \times H$ is not DRR-detecting.

Case 2. $|G|$ is divisible by precisely two distinct primes p and q. Since G is nilpotent, we have $G = P \times Q$, where P is a Sylow p-subgroup and Q is a Sylow q-subgroup of G. If P and Q each admit a DRR, then Theorem 1.9 implies that $G = P \times Q$ is not DRR-detecting.

We may thus assume, without loss of generality, that P does not admit a DRR. Using Theorem 2.3 and Lemma 6.1 and interchanging P and Q if necessary, we may assume that P is isomorphic to one of $(\mathbb{Z}_2)^2$, $(\mathbb{Z}_2)^3$, $(\mathbb{Z}_2)^4$, or $(\mathbb{Z}_3)^2$. Thus, we may write $P = (\mathbb{Z}_p)^r$, with $r \geq 2$.

Since $(\mathbb{Z}_p)^{r-1} \times Q$ is not a p-group, we may assume, by induction on $|G|$, that it is not DRR-detecting. Also note that $\mathbb{Z}_p$ admits a DRR. (Take the directed p-cycle $\overrightarrow{C_p}$ if $p \geq 3$; or take K_2 if $p = 2$.) Therefore, by applying Theorem 1.10 with $G_1 = \mathbb{Z}_p$ and $G_2 = (\mathbb{Z}_p)^{r-1} \times Q$, we see that the group $G = \mathbb{Z}_p \times \big((\mathbb{Z}_p)^{r-1} \times Q\big)$ is not DRR-detecting. □

Acknowledgments. This work was supported in part by the Natural Science and Engineering Research Council of Canada (grant RGPIN-2017-04905), and Gabriel Verret is grateful to the N.Z. Marsden Fund for its support (via grant UOA1824). We thank two anonymous referees for helpful comments.

References

[1] L. Babai. Finite digraphs with given regular automorphism groups. *Periodica Mathematica Hungarica* **11** (1980), 257–270. `https://doi.org/10.1007/BF02107568`

[2] J. Dixon, B. Mortimer. Permutation Groups. Graduate texts in Mathematics, 163. *Springer-Verlag, New York*. 1996. `https://doi.org/10.1007/978-1-4612-0731-3`

[3] E. Dobson, J. Morris. Automorphism groups of wreath product digraphs. *Electronic. J. Combin.* **16** (2009), #R17. `https://doi.org/10.37236/106`

[4] C. Godsil. GRRs for nonsolvable groups. *Algebraic Methods in Graph Theory, Vol. I, II (Szeged, 1978)*, pp. 221–239. North-Holland, Amsterdam, 1981.

[5] C. Godsil. On the full automorphism group of a graph. *Combinatorica* **1** (1981), 243–256. `https://doi.org/10.1007/BF02579330`

[6] M. Grech, W. Imrich, A. D. Krystek, L. J. Wojakowski. Direct product of automorphism groups of digraphs. *Ars Math. Contemp.* **17** (2019), 89–101. `https://doi.org/10.26493/1855-3974.1498.77b`

[7] W. Imrich. On products of graphs and regular groups. *Israel J. Math* **11** (1972), 258–264. `https://doi.org/10.1007/BF02789317`

[8] L. Morgan, J. Morris, G. Verret. Digraphs with small automorphism groups that are Cayley on two nonisomorphic groups. *Art of Discrete and Applied Math.* 3 (2020) #P1.01. `https://doi.org/10.26493/2590-9770.1254.266`

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

[10] J.–P. Serre. Linear Representations of Finite Groups. Graduate Texts in Mathematics, 42. *Springer-Verlag, New York*. 1977. `https://doi.org/10.1007/978-1-4684-9458-7`

[11] J. W. Walker. Strict refinement for graphs and digraphs. *J. Combin. Theory Ser. B* **43** (1987), 140–150. `https://doi.org/10.1016/0095-8956(87)90018-9`

[12] Wikipedia. Group cohomology. `https://en.wikipedia.org/wiki/Group_cohomology`