Detecting Graphical and Digraphical Regular Representations in Groups of Squarefree Order

Joy Morris[a] Gabriel Verret[b]

Submitted: Oct 16, 2023; Accepted: Feb 3, 2025; Published: Jun 6, 2025

Abstract

A necessary condition for a Cayley digraph $\mathrm{Cay}(R, S)$ to be a regular representation is that there are no non-trivial group automorphisms of R that fix S setwise. A group is DRR-detecting or GRR-detecting if this condition is also sufficient for all Cayley digraphs or graphs on the group, respectively. In this paper, we determine precisely which groups of squarefree order are DRR-detecting, and which are GRR-detecting.

Mathematics Subject Classifications: 05C25

1 Introduction and background

All groups and digraphs in this paper are finite. Given a group R and a subset $S \subseteq R$, the *Cayley digraph* $\mathrm{Cay}(R, S)$ is the digraph with vertex-set R, with an arc from r to sr if and only if $s \in S$. If $S = S^{-1}$ then we also say that $\mathrm{Cay}(R, S)$ is a *Cayley graph*. It is straightforward to show that the right-regular representation $\hat{R}$ of R is a subgroup of the automorphism group of $\mathrm{Cay}(R, S)$. It is also not hard to show that, conversely, if the automorphism group of a digraph admits a regular subgroup isomorphic to R, then the digraph is isomorphic to $\mathrm{Cay}(R, S)$ for some $S \subseteq R$. Digraphs such that their (full) automorphism group is regular are of special interest.

Definition 1. A Cayley digraph $\mathrm{Cay}(R, S)$ is a *Digraphical Regular Representation* (*DRR* for short) if $\mathrm{Aut}(\mathrm{Cay}(R, S)) = \hat{R}$. If it is also a Cayley graph, then it is a *Graphical Regular Representation* or *GRR*.

It is usually not easy to determine whether a Cayley digraph is a DRR, mostly because it is not easy to calculate the automorphism group. On the other hand, there is a particular

[a]Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB. T1K 3M4, Canada (joy.morris@uleth.ca).
[b]Department of Mathematics, University of Auckland, 38 Princes Street, 1010 Auckland, New Zealand (g.verret@auckland.ac.nz).

subgroup of the automorphism group that is easier to understand. We first introduce some notation. Given a permutation group G acting on a set Ω and $S \subseteq \Omega$, we denote by G_S the subgroup of G that fixes S setwise. Given two subgroups X and Y of a common overgroup, we denote by $\mathbf{N}_Y(X)$ ($\mathbf{C}_Y(X)$) the normaliser (centraliser) of X in Y.

Theorem 2. *[5, Lemma 2.1] Let R be a group, let $S \subseteq R$ and let $A = \mathrm{Aut}(\mathrm{Cay}(R, S))$. Then $\mathbf{N}_A(\hat{R}) = \hat{R} \rtimes \mathrm{Aut}(R)_S$.*

Generally speaking, given a Cayley digraph $\mathrm{Cay}(R, S)$, calculating $\hat{R} \rtimes \mathrm{Aut}(R)_S$ is relatively easy, especially compared to determining $\mathrm{Aut}(\mathrm{Cay}(R, S))$. We are interested in groups for which knowing $\hat{R} \rtimes \mathrm{Aut}(R)_S$ is enough to decide whether $\mathrm{Cay}(R, S)$ is a DRR.

Definition 3. A group R is *DRR-detecting* if, for every subset S of R, $\mathrm{Aut}(R)_S = 1$ implies that $\mathrm{Cay}(R, S)$ is a DRR. It is *GRR-detecting* if, for every inverse-closed subset S of R, $\mathrm{Aut}(R)_S = 1$ implies that $\mathrm{Cay}(R, S)$ is a GRR.

Clearly, every DRR-detecting group is GRR-detecting. If $\mathrm{Aut}(R)_S = 1$ but $\mathrm{Cay}(R, S)$ is not a DRR (respectively, not a GRR), then we say that $\mathrm{Cay}(R, S)$ *witnesses that R is not DRR-detecting* (respectively, *not GRR-detecting*). Equivalently by Theorem 2, $\mathrm{Cay}(R, S)$ witnesses that R is not DRR-detecting if $\hat{R}$ is self-normalising in $\mathrm{Aut}(\mathrm{Cay}(R, S))$ but $\mathrm{Cay}(R, S)$ is not a DRR.

We would like to determine which groups are DRR-detecting or GRR-detecting. Previous work on this topic includes a result by Godsil [5] that if p is prime, then every p-group that admits no homomorphism onto the wreath product $\mathrm{C}_p \wr \mathrm{C}_p$ is DRR-detecting. In particular, every abelian p-group is DRR-detecting. In [12], with D. Morris we showed that this result is sharp in the sense that $\mathrm{C}_p \wr \mathrm{C}_p$ is not GRR-detecting (or DRR-detecting) when p is odd. We also proved that if a DRR-detecting group is nilpotent, then it is a p-group. In this paper we determine which groups of squarefree order are GRR-detecting, and which are DRR-detecting:

Theorem 4. *Let R be a group of squarefree order.*

1. *If $|R|$ is prime, then R is DRR-detecting (and therefore is GRR-detecting).*
2. *If $|R|$ has two prime factors, then:*
   - *(a) R is not GRR-detecting (and therefore not DRR-detecting) if $R \cong \mathrm{C}_q \rtimes \mathrm{C}_r$ and either:*
     - *i. $(q, r) = (31, 5)$; or*
     - *ii. (q, r) is a safe/Sophie Germain prime pair with $q \equiv 3 \pmod 4$ and $q \geqslant 11$.*
   - *(b) R is GRR-detecting but not DRR-detecting if:*
     - *i. R is abelian; or*
     - *ii. $R \cong \mathrm{C}_7 \rtimes \mathrm{C}_3$.*
   - *(c) R is DRR-detecting (and therefore GRR-detecting) if R does not fall into any of the above cases.*

3. *If $|R|$ has at least three prime factors, then R is not DRR-detecting, but is GRR-detecting if one of the following holds:*

   (a) *R is abelian;*

   (b) *$R \cong \mathrm{D}_{30}$; or*

   (c) *$R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$ with $r \in \{3, 5\}$.*

(Throughout the paper, C_n denotes a cyclic group of order n and D_{2n} a dihedral group of order $2n$. A safe/Sophie Germain prime pair is a pair of primes (q, r) such that $q = 2r + 1$.)

In Section 2, we define generalised wreath products in the context of Cayley digraphs and show that they are never DRRs, which makes them very useful as potential witnesses that a group is not DRR-detecting (or GRR-detecting). We also give a sufficient condition to recognise a Cayley digraph as a generalised wreath product. Starting in Section 3, we restrict our attention to groups of squarefree order. We first show that "most" of these groups are not GRR-detecting and then deal with the remaining "exceptional" groups in Section 4.

2 Generalised wreath products

Our main approach to construct witnesses is to use generalised wreath products. It is therefore important for us to understand what a generalised wreath product is in the context of Cayley digraphs.

Definition 5. Let R be a group and let $S \subseteq R$. If there exist K and H with $1 < K \trianglelefteq H < R$ such that

$$K(S \setminus H) = S \setminus H = (S \setminus H)K \tag{$\star\star$}$$

then $\mathrm{Cay}(R, S)$ is a *nontrivial generalised wreath product (with respect to K and H)*. If $H = K$, then $\mathrm{Cay}(R, S)$ is a *nontrivial wreath product (with respect to K)*.

It is not hard to see that, if $K \trianglelefteq R$ or $S = S^{-1}$, then ($\star\star$) is equivalent to $K(S \setminus H) = S \setminus H$. We will often use this fact throughout the paper.

Lemma 6. *A Cayley digraph that is a nontrivial generalised wreath product is not a DRR.*

Proof. Let $\Gamma = \mathrm{Cay}(R, S)$ be a nontrivial generalised wreath product with respect to K and H. By definition, we have $1 < K \trianglelefteq H < R$ and $K(S \setminus H) = S \setminus H = (S \setminus H)K$.

Let $k \in K$ and let $\alpha_k \in \mathrm{Sym}(R)$ be the map which right multiplies elements of H by k while fixing all other elements of R. We claim that $\alpha_k \in \mathrm{Aut}(\Gamma)$. Let (y, x) be an arc of Γ, so that $xy^{-1} \in S$. We check that $\alpha_k(x)\alpha_k(y)^{-1} \in S$. If $x, y \notin H$, this is trivial. Similarly, if $x, y \in H$, then $\alpha_k(x)\alpha_k(y)^{-1} = xk(yk)^{-1} = xy^{-1} \in S$. Now, suppose that $x \in H$ and $y \notin H$. In particular, $xy^{-1} \notin H$. We have

$$\alpha_k(x)\alpha_k(y)^{-1} = xky^{-1} = k^{x^{-1}}xy^{-1} \in Kxy^{-1} \subseteq K(S \setminus H) = S \setminus H,$$

as required (we used the fact that $K \trianglelefteq H$ and $x \in H$). Finally, if $x \notin H$ and $y \in H$, then again $xy^{-1} \notin H$ and

$$\alpha_k(x)\alpha_k(y)^{-1} = x(yk)^{-1} = xk^{-1}y^{-1} = xy^{-1}(k^{-1})^{y^{-1}} \in xy^{-1}K \subseteq (S \setminus H)K = S \setminus H.$$

Since $1 < K$, there is some k such that $\alpha_k \neq 1$ and, since $H < R$, it follows that $\alpha_k \notin \hat{R}$ and Γ is not a DRR. □

We have the following immediate corollary.

Corollary 7. *Let R be a group, let $S \subseteq R$ and let K and H be such that*

1. $1 < K \trianglelefteq H < R$,
2. $K(S \setminus H) = S \setminus H = (S \setminus H)K$, *and*
3. $\mathrm{Aut}(R)_S = 1$.

Then $\mathrm{Cay}(R, S)$ *witnesses that R is not DRR-detecting (and not GRR-detecting if $S = S^{-1}$).*

To apply Corollary 7, one must show that $\mathrm{Aut}(R)_S = 1$. To do this, it will often be easiest to show first that $\mathrm{Aut}(R)_S$ normalises H, so that $\mathrm{Aut}(R)_S = \mathrm{Aut}(R)_{S \cap H} \cap \mathrm{Aut}(R)_{S \setminus H}$. The most obvious situation in which $\mathrm{Aut}(R)_S$ normalises H is if $\mathrm{Aut}(R)$ itself normalises H; that is, when H is characteristic in R. Here is another approach that can also be used.

Proposition 8. *Let R be a group, let $S \subseteq R$ and let $1 < K < H < R$. If*

1. *K is characteristic in R,*
2. *K is maximal in H,*
3. *$K(S \setminus H) = S \setminus H$, and*
4. *it is not the case that $K(S \setminus K) = S \setminus K$,*

then $\mathrm{Aut}(R)_S$ *normalises H.*

Proof. Let $H_0 = \langle s \in S : Ks \not\subseteq S \rangle$. Since K is characteristic in R, $\mathrm{Aut}(R)$ normalises K, and therefore so does $\mathrm{Aut}(R)_S$. It follows that $\mathrm{Aut}(R)_S$ normalises H_0. By (3) we have $H_0 \leqslant H$, and by (4), $H_0 \not\leqslant K$. It follows that $K < KH_0 \leqslant H$. Since K is maximal in H, $H = KH_0$ hence $\mathrm{Aut}(R)_S$ normalises H, as required. □

We end this section with a sufficient condition to recognise a Cayley digraph as a nontrivial generalised wreath product. (For $G \leqslant \mathrm{Aut}(\mathrm{Cay}(R, S))$, we denote by G_1 the stabiliser of the vertex of $\mathrm{Cay}(R, S)$ corresponding to the identity of R.)

Lemma 9. *Let R be a group, let $S \subseteq R$, let $G \leqslant \mathrm{Aut}(\mathrm{Cay}(R,S))$ and let K and H be such that $1 < K \trianglelefteq H < R$ and $H \leqslant \mathbf{N}_R(G_1)$. If, for every $r \in R \setminus H$, we have $K, K^r \subseteq G_1 G_1^r$, then $\mathrm{Cay}(R,S)$ is a nontrivial generalised wreath product with respect to K and H. Moreover, if $S = S^{-1}$, then $K \subseteq G_1 G_1^r$ is sufficient to reach the same conclusion.*

Proof. Since $H \leqslant \mathbf{N}_R(G_1)$, we have $G_1 H^{G_1} = G_1 H G_1 = G_1 H$. Note that since $G \leqslant \mathrm{Aut}(\mathrm{Cay}(R,S))$ implies that $S^{G_1} = S$, we have $G_1(S \setminus H)^{G_1} = G_1(S \setminus H)$. If, for every $r \in R \setminus H$, we have $K \subseteq G_1 G_1^r$, then we have

$$G_1 K r^{-1} \subseteq G_1 G_1^r r^{-1} = G_1 r^{-1} G_1 = G_1 (r^{-1})^{G_1}$$

and it follows that $G_1 K(S \setminus H) \subseteq G_1(S \setminus H)^{G_1} = G_1(S \setminus H)$. Since $G_1 \cap (K(S \setminus H)) = 1$, this implies $K(S \setminus H) = S \setminus H$. Likewise, if for every $r \in R \setminus H$, we have $K^r \subseteq G_1 G_1^r$, then

$$G_1 r^{-1} K \subseteq G_1 r^{-1} G_1 = G_1 (r^{-1})^{G_1}$$

and it follows that $G_1(S \setminus H)K \subseteq G_1(S \setminus H)^{G_1} = G_1(S \setminus H)$, which again implies $(S \setminus H)K = S \setminus H$.

Hence, if $K, K^r \subseteq G_1 G_1^r$ for every $r \in R \setminus H$, then $K(S \setminus H) = S \setminus H = (S \setminus H)K$ hence $\mathrm{Cay}(R,S)$ is a nontrivial generalised wreath product. Moreover, if $S = S^{-1}$, then as previously noted, $K(S \setminus H) = S \setminus H$ suffices to reach the same conclusion. □

3 Groups of squarefree order, generic case

The structure of groups of squarefree order has been well understood since the work of Hölder [7]. An obvious observation is that every subgroup of such a group is a Hall subgroup hence every normal subgroup is characteristic. Hölder proved that these groups are metacyclic. In particular, if R is a group of squarefree order, we have $R \cong \mathrm{C}_t \times (\mathrm{C}_n \rtimes \mathrm{C}_m)$, where $\mathrm{Z}(\mathrm{C}_n \rtimes \mathrm{C}_m) = 1$ (and t, n and m are pairwise coprime) see for example [2]. (We use the usual notation $\mathrm{Z}(G)$ for the centre of the group G.) An easy consequence of this is the fact that, for every set of primes π dividing $|R|$, R has a Hall π-subgroup. Finally, we will make frequent use of the fact that if p and q are primes with $q > p$ and X is a nonabelian subgroup of order pq, then $q \equiv 1 \pmod{p}$. We will also make use of the following result.

Lemma 10. *Let $R \cong \mathrm{C}_n \rtimes \mathrm{C}_m$ be a group of squarefree order with trivial center. Suppose that, for every pair of primes p and q with $p \mid m$ and $q \mid n$, every subgroup of R of order pq is nonabelian. Let H be a characteristic subgroup of prime index in R. If m is not prime, then $\mathbf{C}_{\mathrm{Aut}(R)}(H) = 1$.*

Proof. Let x and y be elements of order m and n in R, respectively and let $Y = \langle y \rangle$. Note that Y is a characteristic subgroup of R and there exists an integer j such that, for every $y' \in Y$, we have $(y')^x = (y')^j$. Now, if $\alpha \in \mathrm{Aut}(R)$, then x^α must also have this property, that is, $(y')^{x^\alpha} = (y')^j$ for every $y' \in Y$. An easy calculation shows that this implies that

$x^\alpha \in Yx$, say $x^\alpha = y^i x$. Let $p = |R : H|$. Note that, since H is normal in R, we have $Y \leqslant H$ and p divides m. Let $\alpha \in \mathbf{C}_{\mathrm{Aut}(R)}(H)$. Since m is not prime, we have $x^p \in H \setminus Y$ so $(x^p)^\alpha = x^p$. Since x^p commutes with x, $(x^p)^\alpha = x^p$ commutes with $x^\alpha = y^i x$. It follows that x^p commutes with y^i. If $y^i \neq 1$, then by hypothesis, $\mathbf{C}_R(y^i) = Y$ but $x^p \notin Y$ hence we must have $y^i = 1$. This implies that $x^\alpha = x$ and $\alpha = 1$, as required. □

In our first main result, Theorem 12, we construct Cayley graphs $\mathrm{Cay}(R, S)$ that are nontrivial generalised wreath products with respect to some subgroups K and H of R, and that witness that R is not GRR-detecting. One component of our construction involves taking a GRR on H when possible. In order to understand when this is possible, we will look at known results about which groups admit GRRs, and restrict our attention to groups of squarefree order. Although many researchers including Watkins, Imrich, Nowitz, and Hetzel made significant contributions along the way (see for example [6, 8, 9, 13, 16, 17, 18]), the ultimate result about which groups admit GRRs is due to Godsil. We provide a statement of his result that makes it easy to see which of the groups that do not admit a GRR have squarefree order.

Theorem 11. *[4] Every group admits a GRR except:*

- *abelian groups of exponent greater than* 2*;*
- *generalised dicyclic groups (which have orders divisible by* 4*);*
- *the dihedral groups* D_6 *and* D_{10}*; and*
- *eleven other small groups, none of whose orders is squarefree.*

It follows that the only nonabelian groups of squarefree order that do not admit a GRR are D_6 and D_{10}. We are now ready to show that "most" groups of squarefree order are not GRR-detecting (and thus not DRR-detecting). (We do set aside a number of special cases for further consideration in Section 4.)

Theorem 12. *Let R be a group of squarefree order. If R is not abelian and $R \notin \{\mathrm{D}_6, \mathrm{D}_{10}, \mathrm{D}_{30}, \mathrm{D}_6 \times \mathrm{C}_q, \mathrm{D}_{10} \times \mathrm{C}_q, \mathrm{C}_q \rtimes \mathrm{C}_p : p, q \text{ primes}\}$, then R is not GRR-detecting.*

Proof. We can assume that $|R|$ has at least three prime divisors, since we have excluded the other possibilities. Let $R \cong \mathrm{C}_t \times (\mathrm{C}_n \rtimes \mathrm{C}_m)$, where $\mathrm{Z}(\mathrm{C}_n \rtimes \mathrm{C}_m) = 1$. Since R is nonabelian, we have $n, m \geqslant 2$. We now split the proof into two cases.

Case 1: For every pair of primes p and q with $p \mid m$ and $q \mid nt$, every subgroup of R of order pq is nonabelian.

In this case, we have $t = 1$. Let p be the smallest prime dividing m. If $m \neq p$, then take H to be the characteristic subgroup of index p in R, so $H \cong \mathrm{C}_n \rtimes \mathrm{C}_{m/p}$, with $m/p \geqslant 3$. In particular, H admits a GRR. Let S be the connection set for a GRR on H. Since H is characteristic in R, there is a natural homomorphism $f : \mathrm{Aut}(R) \to \mathrm{Aut}(H)$. Since $\mathrm{Cay}(H, S)$ is a GRR, we have $f(\mathrm{Aut}(R)_S) \leqslant \mathrm{Aut}(H)_S = 1$. It follows that

$\mathrm{Aut}(R)_S \leqslant \ker(f) = \mathbf{C}_{\mathrm{Aut}(R)}(H)$. By Lemma 10, $\mathbf{C}_{\mathrm{Aut}(R)}(H) = 1$ hence $\mathrm{Aut}(R)_S = 1$ and by Corollary 7 (applied with $K = H$), R is not GRR-detecting.

We may thus assume that $m = p$. Since $|R|$ has at least three prime divisors and $t = 1$, n is not prime. Let q be the largest prime dividing n and write $n = qn'$. Recall that every prime divisor of n must be 1 modulo p. If $p \geqslant 3$, then it immediately follows that $q \geqslant 7$. If $p = 2$, the only other possibility is $(q, n) = (5, 15)$, but this is excluded by our hypothesis, hence $q \geqslant 7$ in either case. Let K be the characteristic subgroup of order q in R, and H a subgroup of order pq. Note that H is nonabelian and, since $q \geqslant 7$, H admits a GRR.

Let $k \in K$ have order q, let $h \in H$ have order p, and let $x \in R \setminus H$ have order n'. Let S' be the connection set for a GRR on H, and let $S = S' \cup Khx \cup K(hx)^{-1}$. Suppose that $K(S \setminus K) = S \setminus K$. Note that $K, S' \subseteq H$ whereas $Khx \cap H = \emptyset = K(hx)^{-1} \cap H$ hence $K(S' \setminus K) = S' \setminus K$ and then Lemma 6 implies that $\mathrm{Cay}(H, S')$ is not a DRR, a contradiction. It follows that $K(S \setminus K) \neq S \setminus K$. Let $\alpha \in \mathrm{Aut}(R)_S$. By Proposition 8, α normalises H, so since $\mathrm{Cay}(H, S \cap H)$ is a GRR, α fixes H pointwise. The neighbourhood of $h \in H$ outside H is $Khxh \cup Kx^{-1} = Kx^{h^{-1}}h^2 \cup Kx^{-1}$, which must therefore be fixed setwise by α.

If $1 \neq k \in K$, then k has order q and since k commutes with x^{-1}, it follows that kx^{-1} has order n. This implies that x^{-1} is the unique element of order n' in Kx^{-1}. If $p = 2$, then $Khxh = Kx^{-1}$, whereas if $p \geqslant 3$, then every element of $Kx^{h^{-1}}h^2$ has order p. Either way, α must fix x^{-1} and thus fix R pointwise so $\alpha = 1$. We conclude that $\mathrm{Aut}(R)_S = 1$ and, by Corollary 7, R is not GRR-detecting.

Case 2: There exists primes p and q with $p \mid m$ and $q \mid nt$ such that R has a cyclic subgroup of order pq.

Choose p and q satisfying the above with p as large as possible. Since R is nonabelian, nt is not prime. Let H be the characteristic subgroup of index p in R. Since nt is not prime, H is not isomorphic to D_6 or D_{10}, hence either H admits a GRR or $H \cong \mathrm{C}_{nt}$.

Let $r = nt/q$. Note that every element of order p in R must act nontrivially on some subgroup of the cyclic subgroup of order r in R. We show that $r > 5$. Suppose, by contradiction, that $r \leqslant 5$. This implies $p = 2$ and $r \in \{3, 5\}$. If $m = p = 2$, then $R \cong \mathrm{D}_{2r} \times \mathrm{C}_q$, a case we have excluded by hypothesis. So $m > p$ and there is a prime p' dividing m with $p' > 2$. Since $r \in \{3, 5\}$, R has a cyclic subgroup of order $p'r$ but this contradicts our choice of p. It follows that $r > 5$.

Let k, g and x be elements of order q, r and p in R, respectively. Let $K = \langle k \rangle$ and $B = \langle kg \rangle$. Note that $B \cong \mathrm{C}_{nt}$ and that K and B are both characteristic in R and contained in H. If H is nonabelian, then take S' to be the connection set for a GRR on H; if $H \cong \mathrm{C}_{nt}$ then take $S' = \{kg, (kg)^{-1}\}$. Let $S = S' \cup Kx^{\pm 1} \cup K(gx)^{\pm 1} \cup K(g^3x)^{\pm 1}$. Note that these really are three distinct cosets of K since $|g| = r > 5$. Note also that $S \cap H = S'$ and that $S \setminus S' \subseteq Bx^{\pm 1}$.

Let $\alpha \in \mathrm{Aut}(R)_S$. Since H is characteristic in R, $H^\alpha = H$ hence $(S')^\alpha = S'$. By our choice of S', it follows that $(kg)^\alpha = (kg)^{\pm 1}$ which implies $g^\alpha = g^{\pm 1}$. Write $x^\alpha = bx^\epsilon$, with

$b \in B$ and $\epsilon = \pm 1$. Note that

$$(g^\alpha)^x = (g^x)^\alpha = (g^\alpha)^{x^\alpha} = (g^\alpha)^{bx^\epsilon} = (g^\alpha)^{x^\epsilon}.$$

This implies that $\epsilon = 1$, so $x^\alpha \in Bx$ and therefore α fixes $Kx \cup Kgx \cup Kg^3x$. Since $K^\alpha = K$, α must permute these three K-cosets. Write $(Kx)^\alpha = Kg^ix$ with $i \in \{0, 1, 3\}$. It follows that $(Kgx)^\alpha = (gKx)^\alpha = g^{\pm 1}Kg^ix = Kg^{i\pm 1}x$ and $i \neq 3$. Moreover, if $i = 1$ then $g^\alpha = g^{-1}$ and α interchanges Kg and Kgx, so must fix Kg^3x, so $Kg^3x = (Kg^3x)^\alpha = Kg^{-3+1}x$ and $g^5 = 1$, contradicting $|g| = r > 5$. It follows that $i = 0$ and α fixes Kx, Kgx, and Kg^3x. Since x and k commute, x is the unique element of order p in Kx, so it is fixed by α. Similarly, gx is the unique element of Kgx whose order is not a multiple of q, so it too is fixed by α hence so is g. It follows that α centralises H and $\alpha = 1$. This shows that $\mathrm{Aut}(R)_S = 1$ and it follows from Corollary 7 that R is not GRR-detecting. □

4 Groups of squarefree order, exceptional cases

In this section we proceed through the groups that were excluded in the hypothesis of Theorem 12. We begin with the three sporadic groups. The following result can be checked by computer.

Proposition 13. D_6 *and* D_{10} *are DRR-detecting (and therefore GRR-detecting).* D_{30} *is GRR-detecting but not DRR-detecting.*

If $D_{30} = \langle x, y \mid x^{15} = y^2 = 1, x^y = x^{-1} \rangle$, then $\mathrm{Cay}(D_{30}, \{x^2, x^3, x^5, x^8, x^{11}, x^{14}, y\})$ is a witness that D_{30} is not DRR-detecting.

We next deal with abelian groups. We divide these into two classes, according to whether or not their order is prime.

Proposition 14. *Groups of prime order are DRR-detecting (so are also GRR-detecting).*

Proof. Let R be a group of prime order and let $S \subseteq R$. It is known that either $\hat{R}$ is normal in $\mathrm{Aut}(\mathrm{Cay}(R, S))$ or $\mathrm{Aut}(\mathrm{Cay}(R, S))$ is doubly transitive (see for example [19, Theorem 11.7]). In the latter case, $\mathrm{Cay}(R, S)$ is a complete graph and $\mathrm{Aut}(\mathrm{Cay}(R, S)) = \mathrm{Sym}(R)$. In either case, $\mathrm{Aut}(R)_S = 1$ implies that $\mathrm{Aut}(\mathrm{Cay}(R, S)) = \hat{R}$, and R is DRR-detecting. □

Proposition 15. *Abelian groups of squarefree composite order are GRR-detecting.*

Proof. Let R be an abelian group of squarefree composite order and let $S \subseteq R$ with $S = S^{-1}$. Inversion is a non-identity automorphism of R that preserves S hence $\mathrm{Aut}(R)_S \neq 1$. This shows that R is GRR-detecting. □

We still need to show that abelian groups of squarefree composite order are not DRR-detecting. In order to do so, we will use the following two results.

Theorem 16. *[12, Theorem 1.9] If G_1 and G_2 are nontrivial groups that admit a DRR (a GRR, respectively) and* $\gcd(|G_1|, |G_2|) = 1$*, then $G_1 \times G_2$ is not DRR-detecting (not GRR-detecting, respectively).*

To apply Theorem 16, we need to understand which groups of squarefree order admit DRRs. We use the following result of Babai.

Theorem 17. *[1, Theorem 2.1] Every group admits a DRR except* C_2^i *for* $2 \leqslant i \leqslant 4$, C_3^2, *and* Q_8. *In particular, every group of squarefree order admits a DRR.*

Corollary 18. *Let* R *be a group of squarefree order. If* R *is abelian of composite order or* $R \cong \mathrm{D}_{2r} \times \mathrm{C}_q$ *with* $r \in \{3, 5\}$ *and* q *prime, then* R *is not DRR-detecting.*

Proof. Note that R is a nontrivial direct product of two groups of coprime squarefree order. The result then follows from Theorems 16 and 17. □

To prove Theorem 4, it remains to show that $\mathrm{C}_q \times \mathrm{D}_6$ and $\mathrm{C}_q \times \mathrm{D}_{10}$ are GRR-detecting and to determine the status of nonabelian groups whose order is a product of two primes. This is our goal in the remainder of the paper.

4.1 The case when $\mathrm{Cay}(R, S)$ is a generalised wreath product

Since we are trying to show that some groups are DRR or GRR-detecting, we have to show that they do not admit witnesses. One case that needs to be handled is to show that even nontrivial generalised wreath products on these groups are not witnesses. This is the goal of this subsection.

Lemma 19. *If* $\mathrm{Cay}(R, S)$ *is a nontrivial generalised wreath product with respect to* K *and* H *and* $\mathrm{Z}(H) \cap K \not\leqslant \mathrm{Z}(R)$, *then* $\mathrm{Aut}(R)_S > 1$.

Proof. By definition, $K(S \setminus H) = S \setminus H = (S \setminus H)K$. Let k be an element of $(\mathrm{Z}(H) \cap K) \setminus \mathrm{Z}(R)$ and let $\alpha_k \in \mathrm{Aut}(R)$ denote conjugation by k. Since $k \in \mathrm{Z}(H)$, we have that α_k fixes H pointwise. Moreover, since $k \in K$, for every $s \in S \setminus H$, we have $s^{\alpha_k} = k^{-1}sk \in KsK \subseteq S$. It follows that $\alpha_k \in \mathrm{Aut}(R)_S$. Finally, as $k \notin \mathrm{Z}(R)$, $\alpha_k \neq 1$, as required. □

From this we are able immediately to prove our desired result in the case where $|R|$ is a product of two primes.

Corollary 20. *Let* R *be a nonabelian group whose order is a product of two distinct primes and let* $S \subseteq R$. *If* $\mathrm{Cay}(R, S)$ *is a nontrivial generalised wreath product, then* $\mathrm{Aut}(R)_S > 1$.

Proof. Say that $\mathrm{Cay}(R, S)$ is a nontrivial generalised wreath product with respect to K and H, so that $1 < K \trianglelefteq H < R$. Given the order of R, we must have $H = K$ of prime order, with $\mathrm{Z}(H) = H \not\leqslant \mathrm{Z}(R) = 1$, and the result follows by Lemma 19. □

It remains to deal with groups of the form $\mathrm{C}_q \times \mathrm{D}_{2r}$ where $r \in \{3, 5\}$. We first need the following result, which is easy but we include a proof for completeness.

Lemma 21. *Let* $r \in \{3, 5\}$, *let* $D = \mathrm{D}_{2r}$ *and let* $S \subseteq D$ *with* $S = S^{-1}$. *Then there exists some nontrivial* $\beta \in \mathrm{Aut}(D)_S$ *that inverts every element of the subgroup of order* r *of* D.

Proof. Let C be the (cyclic) subgroup of order r of D and let $x \in D \setminus C$. We show that there exists an element $z \in xC$ such that conjugation by z fixes S setwise. The result then follows.

Clearly, conjugation by an element of xC inverts every element of C (and hence preserves $S \cap C$), so it suffices to show that $S \setminus C$ is preserved by conjugation by an element of xC. This is equivalent to preserving the complement $(D \setminus C) \setminus (S \setminus C)$. Since $|D \setminus C| \leqslant 5$, we assume without loss of generality that $|S \setminus C| \leqslant 2$.

If $|S \setminus C| = 0$, there is nothing to prove. If $|S \setminus C| = 1$, then just take $z \in S \setminus C$. Finally, assume that $|S \setminus C| = 2$, say $S \setminus C = \{xy^i, xy^j\}$ where $C = \langle y \rangle$. Let $z = xy^{(i+j)/2}$ (where $(i+j)/2$ is computed in $\mathbb{Z}_r$.) One can check that conjugation by z interchanges xy^i and xy^j hence preserves S, as required. □

Proposition 22. *Let $r \in \{3, 5\}$, let q be an odd prime distinct from r, let $R = \mathrm{C}_q \times \mathrm{D}_{2r}$ and let $S \subseteq R$ with $S = S^{-1}$. If $\mathrm{Cay}(R, S)$ is a nontrivial generalised wreath product with respect to K and H, and K has prime order, then $\mathrm{Aut}(R)_S > 1$.*

Proof. Write $R = \langle z \rangle \times (\langle y \rangle \rtimes \langle x \rangle)$, with $|z| = q$, $|y| = r$ and $|x| = 2$. Note that $\mathrm{Z}(R) = \langle z \rangle$. Up to conjugacy, we can assume that K is generated by one of x, y or z. As for H, we can assume that it is maximal in R with respect to being proper in R and normalising K. Indeed, if $\mathrm{Cay}(R, S)$ is a nontrivial generalised wreath product with respect to K and H_0, with $H_0 \leqslant H$, then $S \setminus H_0 = K(S \setminus H_0) = (S \setminus H_0)K$ so $S \setminus H = K(S \setminus H) = (S \setminus H)K$ and $\mathrm{Cay}(R, S)$ is also a nontrivial generalised wreath product with respect to K and H. We thus only have to consider the following cases.

1. $H = \langle x, y \rangle \cong \mathrm{D}_{2r}$ and $K = \langle y \rangle \cong \mathrm{C}_r$;
2. $H = \langle y, z \rangle \cong \mathrm{C}_{qr}$ and $K = \langle y \rangle \cong \mathrm{C}_r$;
3. $H = \langle y, z \rangle \cong \mathrm{C}_{qr}$ and $K = \langle z \rangle \cong \mathrm{C}_q$;
4. $H = \langle x, z \rangle \cong \mathrm{C}_{2q}$ and $K = \langle z \rangle \cong \mathrm{C}_q$; and
5. $H = \langle x, z \rangle \cong \mathrm{C}_{2q}$ and $K = \langle x \rangle \cong \mathrm{C}_2$.

We now address each of these cases individually:

1. $H = \langle x, y \rangle \cong \mathrm{D}_{2r}$ and $K = \langle y \rangle \cong \mathrm{C}_r$. By Lemma 21, there exists some nontrivial $\beta \in \mathrm{Aut}(H)_{S \cap H}$ that acts by inversion on K. In particular $K^\beta = K$. Let α be the unique automorphism of R that fixes z and agrees with β on H. Note that α preserves both K and H so α preserves the two K-cosets in H. If $s \in S \cap H$ then $s^\alpha = s^\beta \in S \cap H$. If $s \in S \setminus H$, say $s \in z^i hK$, for some $h \in H$, then $s^\alpha \in z^i (hK)^\alpha = z^i hK \subseteq S \setminus H$, so $\alpha \in \mathrm{Aut}(R)_S$, as required.
2. $H = \langle y, z \rangle \cong \mathrm{C}_{qr}$ and $K = \langle y \rangle \cong \mathrm{C}_r$. In this case, $\mathrm{Z}(H) \cap K = K \not\leqslant \mathrm{Z}(R)$ and the result follows by Lemma 19.

3. $H = \langle y, z\rangle \cong \mathrm{C}_{qr}$ and $K = \langle z\rangle \cong \mathrm{C}_q$. Let $\pi : R \to R/K$ be the canonical projection mapping. Note that $\pi(R) \cong \mathrm{D}_{2r}$ and $\pi(S) = \pi(S)^{-1}$ so, by Lemma 21, there exists some nontrivial $\beta \in \mathrm{Aut}(\pi(R))_{\pi(S)}$ that inverts every element of $\pi(\langle y\rangle)$. Let α be the unique automorphism of R that inverts z and such that $\pi\beta = \alpha\pi$. (In other words, $s^\alpha K = (sK)^\beta$ for every $s \in R$.) Since H is characteristic in R, we have $H^\alpha = H$. As β inverts $\pi(\langle y\rangle)$, we have $y^\alpha K = (yK)^\beta = y^{-1}K$. Moreover, $\langle y\rangle$ is characteristic in R hence $y^\alpha \in \langle y\rangle \cap y^{-1}K$ and $y^\alpha = y^{-1}$. It follows that α acts by inversion on H. Since $S = S^{-1}$, α preserves $S \cap H$. Now, if $s \in S \setminus H$, then we have $sK \in \pi(S)$ and since β preserves $\pi(S)$, it follows that $s^\alpha K = (sK)^\beta \in \pi(S)$. As $K(S \setminus H) = S \setminus H$, we have that $s^\alpha K \in S \setminus H$. This shows that $\alpha \in \mathrm{Aut}(R)_S$.

4. $H = \langle x, z\rangle \cong \mathrm{C}_{2q}$ and $K = \langle z\rangle \cong \mathrm{C}_q$. Let $\alpha : R \to R$ be defined by $(x^i y^j z^k)^\alpha = x^i y^j z^{-k}$. Note that $\alpha \in \mathrm{Aut}(R)$. Moreover, α acts by inversion on H. Since $S = S^{-1}$, $S \cap H$ is fixed by α. If $s \in S \setminus H$, say $s = x^i y^j z^k$, then $s^\alpha = x^i y^j z^{-k} \in sK \subseteq S \setminus H$ hence $S \setminus H$ is also fixed by α and $\alpha \in \mathrm{Aut}(R)_S$, as required.

5. $H = \langle x, z\rangle \cong \mathrm{C}_{2q}$ and $K = \langle x\rangle \cong \mathrm{C}_2$. In this case, $\mathrm{Z}(H) \cap K = K \not\leq \mathrm{Z}(R)$ and the result follows by Lemma 19. □

4.2 Main results

We are at last ready to show that groups of the form $\mathrm{C}_q \times \mathrm{D}_{2r}$ are GRR-detecting and to characterise DRR-detection and GRR-detection for nonabelian groups whose order is a product of two primes. We first prove the following well known result:

Lemma 23. *If G is a primitive group of affine type with socle an elementary abelian p-group, then a point-stabiliser has no non-trivial normal p-subgroup.*

Proof. Let V be the socle of G and, to arrive at a contradiction let T be a non-trivial normal p-subgroup of G_x. Since T is normal in G_x, $\mathbf{C}_G(T)$ is normalised by G_x. It follows that $Z = \mathbf{C}_V(T)$ is also normalised by G_x. Now, V and T are both p-groups, so $1 < Z$ but since V is a regular subgroup of the permutation group G, $\mathbf{C}_{G_x}(V) = 1 \neq T$ hence $Z < V$. It follows that the orbits of Z form a non-trivial system of imprimitivity for G, contradicting its primitivity. □

The rest of the proof is split into two: Theorem 24 which essentially reduces the problem to the almost simple case, and Corollary 25 which handles that case.

Theorem 24. *Let q, r be distinct primes and either*

- *$r \in \{3, 5\}$, q is odd and let $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, or*
- *R is a nonabelian group isomorphic to $\mathrm{C}_q \rtimes \mathrm{C}_r$.*

Let $S \subseteq R$, suppose that $S = S^{-1}$ when $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$ and let G satisfy $\hat{R} < G \leqslant \mathrm{Aut}(\mathrm{Cay}(R, S))$. If $\hat{R}$ is maximal in G, then one of the following occurs:

1. $\mathrm{Aut}(R)_S > 1$,

2. *$\hat{R}$ is core-free in G and G is almost simple, or*

3. *$R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, C_q is the core of $\hat{R}$ in G, and G/C_q is almost simple.*

Proof. For $X \leqslant \mathrm{Aut}(\mathrm{Cay}(R,S))$, let X_1 denote the stabiliser in X of the vertex of $\mathrm{Cay}(R,S)$ corresponding to the identity of R. For simplicity, we will identify $\hat{R}$ with R from now on. Note that G_1 is non-trivial and core-free in G and $G = RG_1$ with $R \cap G_1 = 1$. Let N be the core of R in G. If R is normal in G, then $1 < G_1 \leqslant \mathrm{Aut}(R)_S$, hence we assume that R is not normal in G and $N < R$. Let $\overline{G} = G/N$, $\overline{R} = R/N$ and $\overline{G_1} = G_1N/N \cong G_1$. Note that $\overline{R}$ is a maximal core-free subgroup of $\overline{G}$, so we can view $\overline{G}$ as a primitive group with point-stabiliser $\overline{R}$ and a regular subgroup $\overline{G_1}$. Since the point-stabiliser $\overline{R}$ is soluble, the primitive type of $\overline{G}$ is either affine, almost simple, or product action. Moreover, because the order of the point-stabiliser $\overline{R}$ is squarefree, the product action case can't occur. (See for example [10, Theorem 1.1] for both of these claims.)

Suppose first that $\overline{G}$ is almost simple. In this case, the point-stabiliser $\overline{R}$ cannot be abelian (see for example [3, Lemma 2.1]), so either $N = 1$ (and $G \cong \overline{G}$, $R \cong \overline{R}$, and conclusion (2) holds, completing the proof) or $N \cong \mathrm{C}_q$ and $\overline{R} \in \{\mathrm{D}_6, \mathrm{D}_{10}\}$. In the latter case, conclusion (3) holds, again completing the proof.

From now on, we assume that $\overline{G}$ is of primitive affine type. In this case, there exists a normal subgroup E of G such that $N \leqslant E$, $\overline{G} = \overline{E} \rtimes \overline{R}$ and $\overline{E} \cong \mathrm{C}_p^x$ for some prime p. It follows that $|G_1| = |\overline{G_1}| = p^x$. Note that $\overline{R}$ acts faithfully and irreducibly on $\overline{E}$. We now prove the following claim.

Claim: If p divides $|N|$ and R has a normal Sylow p-subgroup, then $\mathrm{Aut}(R)_S > 1$.

Let $H = \mathbf{N}_R(G_1)$, let K be a Sylow p-subgroup of R and let X be a Sylow p-subgroup of E. Since p divides $|N|$, it does not divide $|\overline{R}|$, hence $\overline{E}$ is a normal Sylow p-subgroup of $\overline{G}$. Note that K is characteristic in N thus normal in G. It follows that $K \leqslant X$, $X/K = \overline{E}$ and X is normal in G. Moreover, $|X : G_1| = p$, hence G_1 is normal and maximal in X hence $K \leqslant H$. Let $r \in R \setminus H$. By definition, we have $G_1^r \neq G_1$ but G_1 is contained in X which is normal in G, so $G_1^r \leqslant X$. Since G_1 is a normal maximum subgroup of X, $G_1G_1^r = X$. It follows that $K, K^r \subseteq X = G_1G_1^r$, and we can apply Lemma 9 to conclude that $\mathrm{Cay}(R,S)$ is a nontrivial generalised wreath product with respect to K and H. If $R \cong \mathrm{C}_q \rtimes \mathrm{C}_r$ then the claim follows by Corollary 20, whereas if $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, it follows by Proposition 22. □

We split the remainder of the proof into two cases, according to whether N is cyclic or dihedral.

***N* is cyclic:** Suppose that p divides $|N|$. Since N is cyclic, its Sylow p-subgroup is characteristic, therefore normal in R. We can thus apply our claim to conclude that $\mathrm{Aut}(R)_S > 1$, completing the proof. From now on, we assume that p does not divide $|N|$. Let C be the centraliser of N in G. Since N is cyclic, we have $N \leqslant C$. If $N = C$, then G/N embeds in $\mathrm{Aut}(N)$ which is abelian, a contradiction since G/N is nonabelian. We

conclude that $N < C$. Since $\overline{E}$ is the unique minimal normal subgroup of $\overline{G}$, we have $E \leqslant C$.

If p is coprime to $|\overline{R}|$, then $\overline{E}$ is the unique Sylow p-subgroup of $\overline{G}$ so $\overline{G_1} = \overline{E}$ and $G_1 \leqslant E \leqslant C$ which implies $E = NG_1 = N \times G_1$. Since p does not divide $|N|$, G_1 is characteristic in E, and thus normal in G, a contradiction. This shows that p divides $|\overline{R}|$. Recall that $\overline{R}$ has no non-trivial normal p-subgroup (Lemma 23), so we get the following cases:

1. $R \cong \mathrm{C}_q \rtimes \mathrm{C}_r$, $N = 1$, $\overline{R} \cong \mathrm{C}_q \rtimes \mathrm{C}_r$ and $p = r$.
2. $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, $N = 1$, $\overline{R} \cong \mathrm{C}_q \times \mathrm{D}_{2r}$ and $p = 2$.
3. $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, $N \cong \mathrm{C}_q$, $\overline{R} \cong \mathrm{D}_{2r}$ and $p = 2$.

In case (1), we have $G = E \rtimes R \cong \mathrm{C}_r^x \rtimes (\mathrm{C}_q \rtimes \mathrm{C}_r)$. Since $\mathrm{C}_q \rtimes \mathrm{C}_r$ is nonabelian and acts faithfully on C_r^x, we have $x \geqslant 2$ and $E_1 \neq 1$. Since G_1 is not normal in G, we have $G_1 \neq E$, hence $|EG_1 : G_1| = |EG_1 : E| = r$. It follows that both E_1 and G_1 are normal in EG_1. Note that EG_1 is a maximal subgroup of G and neither E_1 nor G_1 is normal in G (since G_1 is core-free in G), so $\mathbf{N}_G(E_1) = \mathbf{N}_G(G_1) = EG_1$. Note that $REG_1 = G$, hence

$$|G| = \frac{|R||EG_1|}{|R \cap EG_1|} = \frac{|R||E||G_1|}{|R \cap EG_1||E \cap G_1|} \qquad (\star)$$

and $|R \cap EG_1| = |G_1 : E \cap G_1| = r$. Let $K = R \cap EG_1 = \mathbf{N}_R(E_1) = \mathbf{N}_R(G_1) \cong \mathrm{C}_r$. By definition, $EK \leqslant EG_1$ hence $EK = EG_1$ by order considerations.

We show that, for every $s \in R \setminus K$, we have $K, K^s \subseteq G_1 G_1^s$. Since $K = \mathbf{N}_R(E_1)$, we have $E_1^s \neq E_1$. Since E_1 is maximal in E which is normal in G, it follows that $E = E_1 E_1^s \subseteq G_1 G_1^s$, so $G_1 G_1^s = EG_1 G_1^s$. Now, $K \leqslant EK = EG_1 \subseteq EG_1 G_1^s = G_1 G_1^s$. On the other hand, since $EK = EG_1$, we have $EG_1^s = EK^s$ and thus $K^s \subseteq EG_1 K^s = EKK^s = EKEK^s = EG_1 EG_1^s = G_1 G_1^s$, as required. It follows by Lemma 9 that $\mathrm{Cay}(R, S)$ is a nontrivial wreath product with respect to K and the claim follows by Corollary 20.

In case (2), we have $G = E \rtimes R \cong \mathrm{C}_2^x \rtimes (\mathrm{C}_q \times \mathrm{D}_{2r})$. We consider faithful irreducible representations of $\mathrm{C}_q \times \mathrm{D}_{2r}$ over $\mathbb{F}_2$. Since $\mathrm{C}_q \times \mathrm{D}_{2r}$ is a direct product, its representations arise as tensor products of the ones for C_q and D_{2r}. Note that the faithful irreducible representations of the factors have dimension at least 2.

Since G_1 is not normal in G, we have $E \neq G_1$ hence $|EG_1 : E| = |EG_1 : G_1| = 2$ and, in particular, $EG_1 \leqslant \mathbf{N}_G(E_1)$. Now, suppose $EG_1 < \mathbf{N}_G(E_1)$, so an element of R of order q or r normalises $E_1 \cong \mathrm{C}_2^{x-1}$. By Maschke's Theorem, it must also normalise some $\mathrm{C}_2 \leqslant E$, but this contradicts the dimensions of the faithful irreducible representations in the previous paragraph. We conclude that $\mathbf{N}_G(E_1) = EG_1$. A calculation similar to $(\star)$ yields that $|R \cap EG_1| = |G_1 : E \cap G_1| = 2$. Let $K = R \cap EG_1 = \mathbf{N}_R(E_1) \leqslant \mathbf{N}_R(G_1)$. Let $r \in R \setminus K$, so $E_1^r \neq E_1$. Since E_1 is normal and maximal in E, which itself is normal in G, it follows that $E_1 E_1^r = E$. It follows that $K \leqslant EG_1 \subseteq G_1 G_1^r$ and, by Lemma 9, $\mathrm{Cay}(R, S)$

is a nontrivial wreath product with respect to K. Note that $K \cong \mathrm{C}_2$, so Proposition 22 completes the proof.

In case (3), $R \leqslant C$, so $G = ER \leqslant C$ and N is central in G hence $G \cong \mathrm{C}_q \times (\mathrm{C}_2^x \rtimes \mathrm{D}_{2r})$. Let $X \cong \mathrm{C}_2^x$ be the Sylow 2-subgroup of E. Note that X is normal in G. Since D_{2r} is nonabelian and acts faithfully on X, we have $x \geqslant 2$ and $X_1 \neq 1$. Since G_1 is not normal in G, we have $G_1 \neq X$, hence $|XG_1 : G_1| = |XG_1 : X| = 2$. It follows that X_1 and G_1 are both normal in XG_1. Clearly, C_q also normalises X_1 and G_1, so $\mathbf{N}_G(X_1)$ and $\mathbf{N}_G(G_1)$ both contain $\mathrm{C}_q \times (X \rtimes \mathrm{C}_2)$ which is a maximal subgroup of G. Since neither X_1 nor G_1 is normal in G (since G_1 is core-free in G), we have $\mathbf{N}_G(X_1) = \mathbf{N}_G(G_1) = \mathrm{C}_q \times (X \rtimes \mathrm{C}_2)$. Let $K = R \cap XG_1$ and $H = \mathbf{N}_R(X_1) = \mathbf{N}_R(G_1)$. We have $K \leqslant H$ and a calculation similar to $(\star)$ gives $|K| = 2$ and $|H| = 2q$ hence $K \cong \mathrm{C}_2$ and $H \cong \mathrm{C}_q \times \mathrm{C}_2$. Let $r \in R \setminus H$, so $X_1^r \neq X_1$. Since X_1 is normal and maximal in X, which itself is normal in G, it follows that $X_1 X_1^r = X$. This implies that $K \subseteq XG_1 \subseteq G_1 G_1^r$ and, by Lemma 9, $\mathrm{Cay}(R, S)$ is a nontrivial generalised wreath product with respect to K and H, so Proposition 22 completes the proof.

***N* is isomorphic to $\mathbf{D_{2r}}$:** In this case, $\overline{R} \cong \mathrm{C}_q$ and $\overline{G} \cong \mathrm{C}_p^x \rtimes \mathrm{C}_q$. Let C be the centraliser of N in G. Note that $C \cap N = 1$, so $CN = C \times N$.

Note that q divides $|C \cap R|$ and thus q divides the order of CN/N, which is a normal subgroup of $\overline{G}$. It follows that $CN/N = \overline{G}$ and thus $G = C \times N$ hence $\overline{G} \cong C$ and $G \cong (\mathrm{C}_p^x \rtimes \mathrm{C}_q) \times \mathrm{D}_{2r}$, with $p \neq q$. Since $|G_1| = p^x$ and G_1 is not normal in G, we must have $p \in \{2, r\}$. By the claim proved earlier, we can assume $p = 2$ and $G \cong (\mathrm{C}_2^x \rtimes \mathrm{C}_q) \times \mathrm{D}_{2r}$. Let $X \cong \mathrm{C}_2^x$ be the Sylow 2-subgroup of C. Note that X is normal in G. Moreover, since C_q acts faithfully on X and $q \geqslant 3$, we have $x \geqslant 2$. Since G_1 is not normal, $G_1 \neq X$ hence $|XG_1 : X| = |XG_1 : G_1| = 2$ and $X_1 \neq 1$. The same calculation as in $(\star)$ gives $|R \cap XG_1| = 2$. Write $\langle k \rangle = R \cap XG_1$. Note that XG_1 is elementary abelian and $XG_1 = G_1 \times \langle k \rangle = X \times \langle k \rangle$. Write $X = X_1 \times \langle y \rangle$. Since XG_1/X_1 is a Klein group, there are three subgroups strictly between X_1 and XG_1, namely X, G_1 and $X_1 \times \langle k \rangle$. As $X_1 \times \langle yk \rangle$ is one of these three subgroups, by elimination, we must have $X_1 \times \langle yk \rangle = G_1$. Let h and m be elements of order r and q in R, respectively. Note that m is central in R while $h^k = h^{-1}$ hence $k^h = kh^2$. Note also that k and h commute with X. We have

$$(G_1)^{h^{-i}} = (X_1\langle yk \rangle)^{h^{-i}} = X_1 \langle yk \rangle^{h^{-i}} = X_1 \langle ykh^{-2i} \rangle.$$

Let $\alpha : R \to R$ be given by $(m^j h^i k^\epsilon)^\alpha = m^{-j} h^i k^\epsilon$. Note that $\alpha \in \mathrm{Aut}(R)$. Moreover, $\alpha \neq 1$ since $q \geqslant 3$. We show that $S^\alpha = S$. Note that α fixes $\langle h, k \rangle$ pointwise. Let $s \in S \setminus \langle h, k \rangle$, say $s = m^j h^i k^\epsilon$, with $m^j \neq 1$. If $\epsilon = 1$, then $s^\alpha = m^{-j} h^i k = s^{-1} \in S^{-1} = S$. We now assume that $\epsilon = 0$ so $s = m^j h^i$. Since $\langle m \rangle \cong \mathrm{C}_q$ acts irreducibly on X and $X_1 \neq 1$, we have $(X_1)^{m^j} \neq X_1$, which implies that $X_1 (X_1)^{m^j} = X$ and thus $G_1 (X_1)^{m^j} = G_1 X_1 (X_1)^{m^j} = G_1 X$. Since $m^j \neq 1$, we have

$$\begin{aligned}
G_1 s G_1 &= G_1 m^j h^i G_1 \\
&= G_1 (G_1)^{h^{-i}m^{-j}} m^j h^i \\
&= G_1 (X_1 \langle ykh^{-2i} \rangle)^{m^{-j}} m^j h^i \\
&= G_1 (X_1)^{m^{-j}} \langle ykh^{-2i} \rangle^{m^{-j}} m^j h^i \\
&= G_1 X \langle ykh^{-2i} \rangle^{m^{-j}} m^j h^i \\
&= G_1 \{m^j h^i, km^j h^i, kh^{-2i} m^j h^i, kkh^{-2i} m^j h^i\} \\
&= G_1 \{m^j h^i, m^j h^{-i} k, m^j h^i k, m^j h^{-i}\}
\end{aligned}$$

Since S is preserved under G_1, we have $m^j h^{-i} \in S$ and $s^\alpha = m^{-j} h^i = (m^j h^{-i})^{-1} \in S^{-1} = S$. This completes the proof that $S^\alpha = S$ hence $\alpha \in \mathrm{Aut}(R)_S > 1$. □

We can now completely determine the DRR and GRR-detecting status of these final two families of groups we have been studying.

Corollary 25. *Let q and r be distinct primes.*

1. *If $R \cong \mathrm{C}_7 \rtimes \mathrm{C}_3$, then R is not DRR-detecting but it is GRR-detecting.*
2. *If $R \cong \mathrm{C}_q \rtimes \mathrm{C}_r$, with $(q, r) = (31, 5)$ or (q, r) a safe/Sophie Germain prime pair, with $q \equiv 3 \pmod 4$ and $q \geqslant 11$, then R is not GRR-detecting (so is not DRR-detecting).*
3. *If R is nonabelian and isomorphic to $\mathrm{C}_q \rtimes \mathrm{C}_r$ but not in the above two cases, then R is DRR-detecting (and is therefore also GRR-detecting).*
4. *If q is odd, $r \in \{3, 5\}$ and $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, then R is GRR-detecting.*

Proof. The statement in (1) can be checked by computer.

In [14, Lemma 3.3], it is shown that there are Cayley graphs on $\mathrm{C}_{31} \rtimes \mathrm{C}_5$ with automorphism group $\mathrm{PSL}(5, 2)$. Note that $\mathrm{C}_{31} \rtimes \mathrm{C}_5$ is self-normalising (even maximal) in $\mathrm{PSL}(5, 2)$.

In [14, Lemma 4.4], it is shown that if $q \geqslant 11$ is a prime (the hypothesis that $q \geqslant 11$ is in the paragraph before the statement of the lemma) with $q \equiv 3 \pmod 4$, then there are Cayley graphs on $\mathrm{C}_q \rtimes \mathrm{C}_{(q-1)/2}$ with automorphism group $\mathrm{PSL}(2, q)$. Note that $\mathrm{C}_q \rtimes \mathrm{C}_{(q-1)/2}$ is self-normalising (even maximal) in $\mathrm{PSL}(2, q)$. Together with the previous paragraph, this gives (2).

It remains to show (3) and (4). Let R be one of the groups appearing in (3) or (4). As in Theorem 24, let $S \subseteq R$, suppose that $S = S^{-1}$ when $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$ and let G satisfy $\hat{R} < G \leqslant \mathrm{Aut}(\mathrm{Cay}(R, S))$, with $\hat{R}$ maximal in G. By Theorem 24, we can assume the following:

- $\hat{R}$ is core-free in G and G is almost simple, or

- $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, C_q is the core of $\hat{R}$ in G, and G/C_q is almost simple.

As in the proof of Theorem 24, we identify $\hat{R}$ with R. Let N be the core of R in G, let $\overline{G} = G/N$, $\overline{R} = R/N$ and $\overline{G_1} = G_1N/N$. Note that $\overline{G}$ is an almost simple group with a maximal core-free subgroup $\overline{R}$ and another subgroup $\overline{G_1}$ such that $\overline{G} = \overline{RG_1}$ and $\overline{R} \cap \overline{G_1} = 1$. We can then view $\overline{G}$ as a primitive group of almost simple type with point-stabiliser $\overline{R}$ having a regular subgroup $\overline{G_1}$. Such groups were classified by Liebeck, Praeger, Saxl in [11, Theorem 1.1 and Tables 16.1-16.3].

When consulting these tables, it is important to remember that our point of view (for the moment) is in some sense "dual" to theirs: $\overline{R}$ is our point-stabiliser so it corresponds to their G_α. The next thing to note is that they do not list all the almost simple groups, but rather just their socles (which they denote L and we will denote $\overline{L}$), and do not give G_α, but rather $G_\alpha \cap L$. Now, $\overline{R}$ has the property that its order is squarefree, a product of at most three primes. This property is clearly preserved under subgroups, hence if G_α has this property, so does $G_\alpha \cap L$. So we can go through their tables and list all such instances. This is the result:

$\overline{L}$	$\overline{R} \cap \overline{L}$	Remark
$\mathrm{Alt}(p)$	$\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2}$	$p \equiv 3 \pmod 4$, $p \neq 7, 11, 23$
$\mathrm{PSL}(2,p)$	$\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2}$	**
$\mathrm{PSL}(2,11)$	$\mathrm{C}_{11} \rtimes \mathrm{C}_5$	
$\mathrm{PSL}(2,23)$	$\mathrm{C}_{23} \rtimes \mathrm{C}_{11}$	
$\mathrm{PSL}(2,59)$	$\mathrm{C}_{59} \rtimes \mathrm{C}_{29}$	
$\mathrm{PSL}(3,3)$	$\mathrm{C}_{13} \rtimes \mathrm{C}_3$	
$\mathrm{PSL}(3,4)$	$\mathrm{C}_7 \rtimes \mathrm{C}_3$	$\overline{G} \geqslant \overline{L}.\mathrm{Sym}(3)$
$\mathrm{PSL}(5,2)$	$\mathrm{C}_{31} \rtimes \mathrm{C}_5$	
$\mathrm{PSU}(3,8)$	$\mathrm{C}_{19} \rtimes \mathrm{C}_3$	$\overline{G} \geqslant \overline{L}.3^2$
M_{23}	$\mathrm{C}_{23} \rtimes \mathrm{C}_{11}$	
M_{23}	$\mathrm{C}_{23} \rtimes \mathrm{C}_{11}$	

** In the corresponding line of [11, Table 16.1], there is a remark that this case does not always occur.

Assume first that $R \cong \mathrm{C}_q \times \mathrm{D}_{2r}$, with $r \in \{3, 5\}$. By Theorem 24, $\overline{R}$ is one of $\mathrm{C}_q \times \mathrm{D}_{2r}$ or D_{2r}. From the table above, we see that $\overline{R} \cap \overline{L}$ is centreless, so either way we must have $\overline{R} \cap \overline{L} = \mathrm{D}_{2r}$. Again from the table above, the only case where this could occur is in the second line with $p = 5$, but then we must have $\overline{G} = \overline{L} \cong \mathrm{PSL}(2,5)$, and one can check that there is no subgroup $\overline{G_1}$ of order 6 in $\mathrm{PSL}(2,5)$ such that $\mathrm{PSL}(2,5) = \overline{G_1}\mathrm{D}_{10}$.

From now on, we assume that $R = \mathrm{C}_q \rtimes \mathrm{C}_r$ and R is core-free, so $G = \overline{G}$, $R = \overline{R}$ and $L = \overline{L}$. Since $|R|$ has two prime divisors and, in the table, $R \cap L$ has at least two prime divisors, we must have $R = R \cap L$ and it follows (given the "dual" point of view of [11]) that $G = L$, so G is simple. This allows us to eliminate the cases which have a remark indicating that $\overline{G} > \overline{L}$, that is lines 7 and 9 in our table. (In other words, we can eliminate the cases when $\overline{L} = \mathrm{PSL}(3,4)$ or $\overline{L} = \mathrm{PSU}(3,8)$.)

Finally, we note that all remaining cases correspond to (2) of our statement (that is, $(q,r) = (31,5)$ or (q,r) is a safe/Sophie Germain prime pair, with $q \equiv 3 \pmod 4$ and

$q \geqslant 11$), except the case $\overline{L} = \mathrm{PSL}(3,3)$, which we deal with now. According to the table, we are considering $\mathrm{PSL}(3,3)$ as a transitive permutation group on $13 \cdot 3$ points. There are two conjugacy classes of subgroups of index $13 \cdot 3$ in $\mathrm{PSL}(3,3)$, but they are fused in $\mathrm{Aut}(\mathrm{PSL}(3,3))$. The corresponding transitive permutation group is not primitive: it admits blocks of size 3. This group has rank 3 and its only non-trivial orbital digraphs are $13\mathrm{K}_3$ and its complement (the complete multipartite graph with 13 parts of size 3). It follows that $\mathrm{Cay}(R,S)$ is a nontrivial wreath product with respect to C_3 and $\mathrm{Aut}(R)_S > 1$ by Corollary 20. This concludes the proof. □

Combining Theorems 12 and 24, Propositions 13, 14 and 15, and Corollaries 18 and 25 yields Theorem 4.

Acknowledgements

The authors would like to thank the anonymous referees for their careful reading of the paper, interesting questions, and helpful suggestions. The first author's work is supported by the Natural Science and Engineering Research Council of Canada (grant RGPIN-2017-04905).

References

[1] L. Babai. Finite digraphs with given regular automorphism groups. *Periodica Mathematica Hungarica* **11** (1980), 257–270.

[2] J. H. Conway, H. Dietrich and E. A. O'Brien, Counting groups: gnus, moas, and other exotica, *Math. Intelligencer* **30** (2008), 6–18.

[3] E. Dobson, P. Spiga, G. Verret. Cayley graphs on abelian groups. *Combinatorica* **36** (2016), 371–393.

[4] C. D. Godsil. GRRs for nonsolvable groups, *Algebraic Methods in Graph Theory,* (Szeged, 1978), 221–239, *Colloq. Math. Soc. János Bolyai* **25**, North-Holland, Amsterdam-New York, 1981.

[5] C. Godsil. On the full automorphism group of a graph. *Combinatorica* **1** (1981), 243–256.

[6] D. Hetzel. Über reguläre graphische darstellung von auflösbaren gruppen. *Technishe Universität*, Berlin, 1976.

[7] O. Hölder. Die Gruppen mit quadratfreier Ordnungszahl. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-Physikalische Klasse, 211–219, 1895.

[8] W. Imrich. Graphen mit transitiver Automorphismengruppe. *Monatsh. Math.* **73** (1969), 341–347.

[9] W. Imrich, M. E. Watkins. On automorphism groups of Cayley graphs. *Periodica Math. Hungarica* **7** (1976), 243–258.

[10] C. H. Li, H. Zhang. The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs. *Proc. Lond. Math. Soc.* **103** (2011), 441–472.

[11] M. W. Liebeck, C. E. Praeger, J. Saxl. Regular subgroups of primitive permutation groups. *Mem. Amer. Math. Soc.* **203** (2010), no. 952.

[12] D. W. Morris, J. Morris, G. Verret. Groups for which it is easy to detect graphical regular representations. *Art of Discrete and Applied Math.* **5** (2022), #P1.07.

[13] L. A. Nowitz, M. E. Watkins. Graphical regular representations of non-abelian groups I, II. *Canadian J. Math.* **24** (1972), 1009–1018.

[14] C. E. Praeger, M. Y. Xu. Vertex-primitive graphs of order a product of two distinct primes. *J. Combin. Theory Ser. B* **59** (1993), 245–266.

[15] G. Sabidussi. The composition of graphs. *Duke Math J.* **26** (1959), 693–696.

[16] M. E. Watkins. On the action of non-Abelian groups on graphs. *J. Combin. Theory Ser. B* **11** (1971), 95–104.

[17] M. E. Watkins. On graphical regular representations of $C_n \times Q$. In *Graph theory and applications*, *Lecture Notes in Math.* **303**, Springer, Berlin-New York (1972), 305–311.

[18] M. E. Watkins. Graphical regular representations of alternating, symmetric, and miscellaneous small groups. *Aequationes Math.*, **11** (1974), 40–50.

[19] H. Wielandt. Finite Permutation Groups. Academic Press, New York-London. 1964.