# AUTOMORPHISMS OF CAYLEY GRAPHS ON GENERALISED DICYCLIC GROUPS

JOY MORRIS, PABLO SPIGA, AND GABRIEL VERRET

Abstract. A graph is called a *GRR* if its automorphism group acts regularly on its vertex-set. Such a graph is necessarily a Cayley graph. Godsil has shown that there are only two infinite families of finite groups that do not admit GRRs: abelian groups and generalised dicyclic groups [4]. Indeed, any Cayley graph on such a group admits specific additional graph automorphisms that depend only on the group. Recently, Dobson and the last two authors showed that almost all Cayley graphs on abelian groups admit no automorphisms other than these obvious necessary ones [3]. In this paper, we prove the analogous result for Cayley graphs on the remaining family of exceptional groups: generalised dicyclic groups.

## 1. Introduction

In this paper, all groups considered are finite and all graphs are finite, undirected, and have no multiple edges. (They may have loops and they may be disconnected.) Let $R$ be a group and let $S$ be an inverse-closed subset of $G$. The *Cayley graph* on $R$ with connection set $S$, denoted $\mathrm{Cay}(R,S)$, is the graph with vertex-set $R$ and with $\{g,h\}$ being an edge if and only if $gh^{-1} \in S$. It is easy to check that $R$ acts regularly, by right multiplication, as a group of automorphisms of $\mathrm{Cay}(R,S)$. If, in fact, $R$ is the full automorphism group of $\mathrm{Cay}(R,S)$ then $\mathrm{Cay}(R,S)$ is called a *GRR* (for graphical regular representation).

The most natural question concerning GRRs is to determine which groups admit GRRs. This question was answered by Godsil [4], after a long series of partial results by various authors (see [5, 6, 13] for example).

It turns out that there are only two infinite families of groups which do not admit GRRs. The first family consists of abelian groups of exponent greater than two. If $A$ is such a group and $\iota$ is the automorphism of $A$ mapping every element to its inverse then every Cayley graph on $A$ admits

2010 *Mathematics Subject Classification.* Primary 20B25; Secondary 05E18.

*Key words and phrases.* Cayley graph, dicyclic group, graphical regular representation.

The first author is supported in part by the National Science and Engineering Research Council of Canada. The third author is supported by UWA as part of the Australian Research Council grant DE130101001.

Address correspondence to Gabriel Verret (gabriel.verret@uwa.edu.au).

$A \rtimes \langle \iota \rangle$ as a group of automorphisms. Since $A$ has exponent greater than 2, $\iota \neq 1$ and hence no Cayley graph on $A$ is a GRR.

The other groups that do not admit GRRs are the generalised dicyclic groups, which we now define.

**Definition 1.1.** Let $A$ be an abelian group of even order and of exponent greater than 2, and let $y$ be an involution of $A$. The *generalised dicyclic group* $\mathrm{Dic}(A, y, x)$ is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A\rangle$. A group is called *generalised dicyclic* if it is isomorphic to some $\mathrm{Dic}(A, y, x)$. When $A$ is cyclic, $\mathrm{Dic}(A, y, x)$ is called a *dicyclic* or *generalised quaternion group.*

The importance of generalised dicyclic groups in this context stems from the fact that, just like abelian groups, they admit a non-trivial group automorphism $\iota$ that maps every group element either to itself or to its inverse. More details on this and other basic facts concerning generalised dicyclic groups can be found in Subsection 2.1. For the moment, it suffices to observe that the existence of this group automorphism $\iota$ implies that no Cayley graph on a generalised dicyclic group is a GRR.

As mentioned earlier, it was proved by Godsil that abelian and generalised dicyclic groups are the only two infinite families of groups which do not admit GRRs. The stronger conjecture that follows was made by Babai, Godsil, Imrich and Lovász [1, Conjecture 2.1].

**Conjecture 1.2.** *Let $R$ be a group of order $n$ which is neither generalised dicyclic nor abelian. The proportion of inverse-closed subsets $S$ of $R$ such that* $\mathrm{Cay}(R, S)$ *is a GRR goes to* 1 *as $n \to \infty$.*

Conjecture 1.2 has been verified in the case that $R$ is nilpotent of odd order by Babai and Godsil [1, Theorem 2.2].

If $A$ is abelian then, as we remarked earlier, the smallest possible automorphism group of a Cayley graph on $A$ is $A \rtimes \langle \iota \rangle$. It is then natural to conjecture (as did Babai and Godsil [1, Remark 4.2]) that almost all Cayley graphs on $A$ have automorphism group $A \rtimes \langle \iota \rangle$. This conjecture was recently proved by Dobson and the last two authors.

**Theorem 1.3.** ([3, Theorem 1.5]) *Let $A$ be an abelian group of order $n$. The proportion of inverse-closed subsets $S$ of $A$ such that* $\mathrm{Aut}(\mathrm{Cay}(A, S)) = A \rtimes \langle \iota \rangle$ *goes to* 1 *as $n \to \infty$.*

We now turn our attention to the other exceptional family in Conjecture 1.2, namely the family of generalised dicyclic groups. The situation in this case is slightly more delicate, as this exceptional family contains an even more exceptional sub-family, as we now explain.

Recall that, if $R$ is a generalised dicyclic group then every Cayley graph on $R$ admits $R \rtimes \langle \iota \rangle$ as a group of automorphisms. One might be tempted to conjecture that, as in the abelian case, almost all Cayley graphs on $R$ have $R \rtimes \langle \iota \rangle$ as their full automorphism group. It turns out that this is not the case. Indeed, if $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ (where $\mathrm{Q}_8$ denotes the quaternion group of order 8 and $\mathrm{C}_2$ the cyclic group of order 2) then there exists a permutation group $B$ containing $R$ as a regular subgroup of index 8 and such that every Cayley graph on $R$ admits $B$ as a group of automorphisms. (See Notation 4.1 for the definition of $B$ and Lemma 4.2 for a proof of this fact.)

Our main result is that almost all Cayley graphs on generalised dicyclic groups have automorphism group as small as possible, in the sense of the previous paragraph. More precisely, we prove the following.

**Theorem 1.4.** *Let $R$ be a generalised dicyclic group of order $n$, let $B = R \rtimes \langle \iota \rangle$ if $R \not\cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ and let $B$ be as in Notation 4.1 if $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$. The proportion of inverse-closed subsets $S$ of $R$ such that $\mathrm{Aut}(\mathrm{Cay}(R,S)) = B$ goes to 1 as $n \to \infty$.*

Theorem 1.4 immediately follows from Theorems 3.5 and 4.4. In our proof of Theorem 1.4 we do not make any effort to keep track of the error terms in our estimates. By being more careful, one may obtain the following two more explicit versions of Theorem 1.4.

**Theorem 1.5.** *Let $R$ be a generalised dihedral group of order $n$ with $R \not\cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ and let $m$ be the number of elements of order at most 2 of $R$. Then $R$ has $2^{m/2+n/2}$ inverse-closed subsets and the number of inverse-closed subsets $S$ with $\mathrm{Aut}(\mathrm{Cay}(R,S)) > R \rtimes \langle \iota \rangle$ is at most $(2^{m/2+n/2}) \cdot \varepsilon$ where*

$$\varepsilon \quad = \quad 2^{-n/48+2(\log_2(n))^2+4}.$$

**Theorem 1.6.** *Assume Notation 4.1. Then $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$, $|R| = n$, $R$ has $2^{5n/8}$ inverse-closed subsets and the number of inverse-closed subsets $S$ with $\mathrm{Aut}(\mathrm{Cay}(R,S)) > B$ is at most $(2^{5n/8}) \cdot \varepsilon$ where*

$$\varepsilon \quad = \quad 2^{-n/512+(\log_2(n))^2+2}.$$

We now give a brief summary of the rest of the paper. In Section 2, we establish some basic preliminary results. The case $R \not\cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ of Theorem 1.4 is dealt with in Section 3 while the case $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ is proven in Section 4. In Section 5, we show that the corresponding version of our results for unlabelled graphs easily follows, and give a version of our results for Cayley digraphs. Finally, we use Theorem 3.4 in Section 3 but its proof is technical and of a different flavor than the rest of the paper, so it is delayed to Section 6.

## 2. Preliminaries

Throughout the paper, we denote by $\mathrm{C}_n$ a cyclic group of order $n$, by $\mathrm{D}_n$ a dihedral group of order $2n$ and by $\mathrm{Q}_8$ the quaternion group of order 8. We say that a group $D$ is a *generalised dihedral group* on $A$ if $A$ is an abelian subgroup of $D$ of index 2 and there exists an involution $w \in D \setminus A$ with $a^w = a^{-1}$ for every $a \in A$.

2.1. **Generalised dicyclic groups.** We now establish some basic properties of generalised dicyclic groups. A reader familiar with these groups can probably skip this subsection with little loss.

**Notation 2.1.** Let $A$ be an abelian group of even order and of exponent greater than 2, let $y$ be an involution in $A$ and let $R = \mathrm{Dic}(A, y, x)$. Let $\iota : R \to R$ be the permutation of $R$ fixing $A$ pointwise and mapping every element of $R \setminus A$ to its inverse.

We first mention a few basic properties of $R$ which will be used repeatedly and without comment. (The proofs follow immediately from the definitions.)

**Lemma 2.2.** *Assume Notation* 2.1. *Then the following hold.*

(1) *$\iota$ is an automorphism of $R$.*
(2) *$\langle y\rangle$ is a characteristic subgroup of $R$.*
(3) *Every element in $R \setminus A$ has order* 4 *and squares to $y$.*
(4) *Every subgroup of $R$ is either abelian or generalised dicyclic.*
(5) *The centre of $R$ consists of the elements of $A$ of order at most* 2.
(6) *$R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ if and only if $A \cong \mathrm{C}_4 \times \mathrm{C}_2^\ell$ and $y$ is the unique non-identity square in $A$.*

We also prove some slightly less trivial results.

**Lemma 2.3.** *Assume Notation* 2.1 *and $R \ncong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$.*

(1) *Let $b \in A$ and let $X = \{a \in A \mid a^2 \in \{b, by\}\}$. Then $|X| \leq 2|A|/3$.*
(2) *Let $U < A$ and let $X = \{a \in A \mid a \notin U, a^2 \neq y\}$. Then $|X| \geq |A|/4$.*

*Proof.* Let $A_2 = \{a \in A \mid a^2 = 1\}$. As $A$ is abelian, if $a_1, a_2 \in A$ and $a_1^2 = a_2^2$ then $(a_1 a_2^{-1})^2 = 1$. It follows that $A_2$ is a subgroup of $A$ and, since $A$ has exponent greater than 2, in fact $A_2 < A$. Moreover, it also follows that $\{a \in A \mid a^2 = b\}$ and $\{a \in A \mid a^2 = by\}$ are either empty or have cardinality $|A_2|$. In particular, (1) follows when $|A : A_2| \geq 3$. We thus assume that $|A : A_2| \leq 2$ hence $|A : A_2| = 2$ and $A \cong \mathrm{C}_4 \times \mathrm{C}_2^\ell$. Since $R \ncong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$, $y$ is not a square in $A$. It follows that at most one of $b$ and $by$ is a square in $A$ and thus $|X| \leq |A|/2$. This concludes the proof of (1).

If $y$ is not a square in $A$, then $X = A \setminus U$ and (2) follows immediately. We may thus assume that $y = z^2$ for some $z \in A$. The set of elements of $A$ which square to $y$ is exactly $zA_2$. We must thus show that $|U \cup zA_2| \leq 3|A|/4$. If $|A : A_2| \geq 4$ then $|U \cup zA_2| \leq |U| + |zA_2| \leq |A|/2 + |A|/4 = 3|A|/4$. If $|A : A_2| = 3$ then $A \cong \mathrm{C}_3 \times \mathrm{C}_2^\ell$, contradicting the fact that $A$ contains the element $z$ of order 4. We may thus assume that $|A : A_2| = 2$. It follows that $A \cong \mathrm{C}_4 \times \mathrm{C}_2^\ell$ and, since $y$ is a square in $A$, we get $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$, which is a contradiction. □

2.2. **Primitive groups.** In this subsection, we recall some basic facts about primitive permutation groups. For terminology regarding the types of primitive groups, we follow [9]. Three types of primitive groups will be particularly important in this paper.

Let $G$ be a primitive permutation group. The group $G$ is of *affine type* if it contains a regular elementary abelian $p$-group $T$. In this case, $G_1$ acts faithfully and irreducibly on $T$, which is the unique minimal normal subgroup of $G$. The group $G$ is of *almost simple type* if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group $T$. Finally, $G$ is of *product action type* if $G$ is a subgroup of the wreath product $H \,\mathrm{wr}\, \mathrm{Sym}(l)$ endowed with its natural action on $\Delta^l$ with $l \geq 2$ and $H$ an almost simple primitive group on $\Delta$. Furthermore, if $T$ is the socle of $H$ then $G$ has a unique minimal normal subgroup $N$ and $N = T_1 \times \cdots \times T_l$ where $T_i \cong T$ for every $i \in \{1, \ldots, l\}$. Finally, $\mathbf{N}_G(T_i)$ projects surjectively onto $H$ for every $i \in \{1, \ldots, l\}$.

**Lemma 2.4.** *Let $G$ be a primitive permutation group with an abelian point-stabiliser. Then $G$ is of affine type.*

*Proof.* See for example [3, Lemma 2.1]. □

**Lemma 2.5.** *Let $G$ be a primitive permutation group of affine type with point-stabiliser $G_1$ and socle $T$. Then $\mathbf{Z}(G_1)$ is cyclic of order coprime to $|T|$.*

*Proof.* This follows immediately from Schur's lemma. For a complete proof, see for example [11, Theorem 1]. □

**Lemma 2.6.** *A primitive permutation group of almost simple type cannot have a point-stabiliser of exponent dividing 4.*

*Proof.* We argue by contradiction and suppose that $G$ is a primitive permutation group of almost simple type with point-stabiliser $G_1$ a 2-group of exponent at most 4. Since $G_1$ is a non-identity maximal core-free subgroup of $G$, it is self-normalising in $G$ and hence is a Sylow 2-subgroup of $G$.

Let $T$ be the socle of $G$. Inspecting the lists in [8] yields that $T \cong \mathrm{PSL}(2, q)$ for some $q$ and that $T \cap G_1$ is a non-abelian dihedral group of order $q + 1$ or $q - 1$. Since $G_1$ has exponent at most 4 and $T \cap G_1$ is non-abelian, we have $T \cap G_1 \cong \mathrm{D}_4$. In particular $q = 7$ or $q = 9$.

If $T \cong \mathrm{PSL}(2, 7)$ then either $G \cong \mathrm{PSL}(2, 7)$ or $G \cong \mathrm{PGL}(2, 7)$. In the latter case, a Sylow 2-subgroup of $G$ has exponent 8, while in the former case, a Sylow 2-subgroup of $G$ is not maximal in $G$. We thus obtain a contradiction in both cases.

If $T \cong \mathrm{PSL}(2, 9)$ then $T \leq G \leq \mathrm{P\Gamma L}(2, 9)$. In particular, $G$ is isomorphic to one of the following: $\mathrm{PSL}(2, 9)$, $\mathrm{PGL}(2, 9)$, $M_{10}$, $\mathrm{Sym}(6)$ or $\mathrm{P\Gamma L}(2, 9)$. It is straightforward to check that in none of these cases is a Sylow 2-subgroup of $G$ both maximal and of exponent at most 4. This contradiction concludes the proof. □

**Corollary 2.7.** *A primitive permutation group with a point-stabiliser of exponent dividing 4 is of affine type.*

*Proof.* Assume that $G$ is not of affine type and let $G_1$ be a point-stabiliser of $G$. Again, $G_1$ is a Sylow 2-subgroup of $G$ and hence $G$ has odd degree. In particular, by [10, Theorem], $G$ is of almost simple or product action type. By Lemma 2.6, we may assume that $G$ is of product action type.

Let $N$ be the socle of $G$. Then $N \cong T^\ell$ where $T$ is a non-abelian simple group and $\ell \geq 2$, and $N \trianglelefteq G \leq H \operatorname{wr} \operatorname{Sym}(\ell)$, with $T \trianglelefteq H \leq \operatorname{Aut}(T)$. From the structure of primitive groups of product action type, $H$ is a primitive group of almost simple type with point-stabiliser a 2-group isomorphic to a quotient of a subgroup of $G_1$, and hence of exponent dividing 4. This contradicts Lemma 2.6. □

2.3. **Counting lemmas.** We now prove a few basic counting lemmas that will be used repeatedly.

**Lemma 2.8.** *Let $G$ be a group of order $n$. The number of automorphisms of $G$ and the number of subgroups of $G$ are both at most $2^{o(n)}$.*

*Proof.* Clearly, $G$ admits a generating set of size at most $\log_2(n)$ and hence $|\operatorname{Aut}(G)| \leq n^{\log_2(n)} = 2^{o(n)}$. Similarly, any subgroup of $G$ is also at most $\log_2(n)$-generated and thus $G$ has at most $n^{\log_2(n)} = 2^{o(n)}$ subgroups. □

**Lemma 2.9.** *Let $R$ be a group of order $n$, let $m$ be the number of elements of order at most 2 in $R$ and let $M$ be a subgroup of $R$. Then there are at most $2^{m/2+n/2-|M|/2+o(n)}$ inverse-closed subsets $S$ of $R$ such that $\operatorname{Aut}(\operatorname{Cay}(R,S))$ contains a subgroup $G$ with the following properties:*

- *$G$ contains the right regular representation of $R$,*
- *$G$ normalises $M$,*
- *$G_1$ centralises $M$, and*
- *$G_1$ is not contained in the kernel of the action of $G$ on $M$-orbits.*

*Proof.* Let $\Omega$ be the set of right cosets of $G_1$ in $G$. During this proof, we will be using the action of $G_1$ by conjugation on the elements of $M$; to avoid confusion with the action of $G$ on the vertex-set $R$ of $\operatorname{Cay}(R,S)$ we will consider $G$ as a subgroup of $\operatorname{Sym}(\Omega)$. Since $R$ acts regularly on $\Omega$ there is a natural bijection $\varphi$ from $\Omega$ to $R$, where $\varphi(G_1g)$ is the unique element $r \in R$ such that $G_1g = G_1r$.

Since $G_1$ is not contained in the kernel of the action of $G$ on $M$-orbits, there exists $g \in G_1$ such that $(G_1qM)g = G_1rM$ for some $q, r \in R$ with $qM \neq rM$. In particular, $G_1qg = G_1r\bar{m}$ for some $\bar{m} \in M$. The number of choices for each of $qM$ and $rM$ is at most $n/|M|$. We now assume that $qM$ and $rM$ are fixed. The number of inverse-closed subsets of $R \setminus rM$ is at most $2^{m/2+(n-|M|)/2}$ and hence this is an upper bound for the number of choices for $(R \setminus rM) \cap S$.

Since $g$ centralises $M$, we have

$$(G_1qx)g = G_1qxg = G_1qgx = G_1r\bar{m}x$$

for every $x \in M$. Since $g \in G_1$, $g$ must map $qM \cap S$ onto $rM \cap S$. It follows that $rM \cap S = r\bar{m}q^{-1}(qM \cap S)$ and thus $rM \cap S$ is completely determined by $\bar{m}$ and by $qM \cap S$. The number of choices for $\bar{m}$ is at most $|M|$ and thus the number of choices for $S$ is at most

$$(n/|M|)^2 \cdot |M| \cdot 2^{m/2+n/2-|M|/2} \leq 2^{m/2+n/2-|M|/2+o(n)}. \qquad \square$$

## 3. Cayley graphs on $R$ with $R \ncong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$

We first introduce some notation.

**Notation 3.1.** Let $A$ be an abelian group of even order and of exponent greater than 2, let $y$ be an element of order 2 in $A$ and let $R = \mathrm{Dic}(A, y, x)$. Assume that $R \ncong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$. Let $\iota : R \to R$ be the automorphism of $R$ fixing $A$ pointwise and mapping every element of $R \setminus A$ to its inverse. Let $B = R \rtimes \langle \iota \rangle$, let $C = A \times \langle \iota \rangle$ and let $D = A \rtimes \langle \iota x \rangle$. Let $n = |R|$ and let $m$ be the number of elements of order at most 2 in $R$.

Note that $\iota$ fixes every inverse-closed subset of $R$ setwise and hence every Cayley graph on $R$ admits $B$ as a group of automorphisms. The main result of this section is that, in fact, almost all Cayley graphs on $R$ have $B$ as their full automorphism group. Before we state and prove this, we collect a few basic results about $B$, some of which will be used repeatedly.

**Lemma 3.2.** *Assume Notation* 3.1*. Then*

1. *$C$ is abelian.*
2. *Every subgroup of $A$ is normal in $B$.*
3. *$A$, $C$, $D$ and $R$ are the only proper subgroups of $B$ containing $A$.*
4. *$D$ is a generalised dihedral group on $A$ and $A$ is characteristic in $D$.*
5. *If $X \leq R$, $b \in B$ and $X^b \cap X = 1$, then $X = 1$.*
6. *$R$ is characteristic in $B$.*
7. *Let $N$ be a subgroup of index 2 in $B$ such that $N \notin \{C, D\}$. Then $y \in N$ and the orbit of $y$ under* $\mathrm{Aut}(N)$ *has size at most* 2*.*

*Proof.* The proofs of (1–4) follow immediately from the definitions.

Proof of (5): by (2), $X \cap A$ is normal in $B$ and thus $X \cap A = (X \cap A)^b \leq X^b \cap X = 1$. Since $|R : A| = 2$, it follows that $|X| \leq 2$. As every element of $R \setminus A$ has order 4, we have $X \leq A$ and thus $X \cap A = X = 1$.

Proof of (6): by contradiction, suppose that $R'$ is a distinct conjugate subgroup of $R$ in $B$. Since neither $C$ nor $D$ is generalised dicyclic, it follows that $R' \notin \{C, D\}$. By (3), this implies that $A \nleq R'$. Since $|B : R'| = 2$, it follows that $|X : X \cap R'| = 2$ for every $X \in \{A, C, D, R\}$.

Let $d \in (D \setminus A) \cap R'$. Note that $d$ is an involution. Since every involution in $R$ is central, the same holds in $R'$ and thus $d$ is central in $R'$. Note that $C \cap R'$ is an abelian subgroup of index 2 in $R'$ and that $C \cap R'$ and $d$ generate $R'$. It follows that $R'$ is abelian, which is a contradiction.

Proof of (7): let $N$ be a subgroup of index 2 in $B$ such that $N \notin \{C, D\}$. By (3), it follows that $N \cap (R \setminus A) \neq \emptyset$ and $N \cap A$ has index at most 2 in $A$.

Note that the elements of $R \setminus A$ square to $y$ and, in particular, $y \in N$. Note also that all the elements of $D \setminus A$ square to the identity. It follows that any square in $B$ distinct from 1 and $y$ has all of its square roots in $C$, and, since $C$ is abelian, all of these square roots commute with each other.

In particular, if the square roots in $N$ of $y$ do not commute, then $y$ is the unique non-identity square in $N$ whose square roots do not commute, and hence the orbit of $y$ under $\mathrm{Aut}(N)$ has size 1. We may thus assume that the square roots in $N$ of $y$ commute.

Fix $ax \in N \cap (R \setminus A)$ and let $b \in N \cap A$. Note that $ax$ and $bax$ are both square roots in $N$ of $y$ and hence $(ax)(bax) = (bax)(ax)$. With a computation, this yields $b^2 = 1$ and hence $N \cap A$ is an elementary abelian 2-group.

Since $N \cap A$ has index at most 2 in $A$ and $A$ is not an elementary abelian 2-group, it follows that $A \cong \mathrm{C}_4 \times \mathrm{C}_2^i$ for some $i$ and thus $C \cong \mathrm{C}_4 \times \mathrm{C}_2^{i+1}$. This implies that $C$ contains a unique non-identity square $z$. Thus $y$ and $z$ are the only (not necessarily distinct) non-identity squares of $B$, and hence the orbit of $y$ under $\mathrm{Aut}(N)$ has size at most 2. This completes the proof. □

The following lemma will also prove useful.

**Lemma 3.3.** *Assume Notation* 3.1. *Then there are at most* $2^{m/2+23n/48+o(n)}$ *inverse-closed subsets $S$ of $R$ such that* $\mathrm{Aut}(\mathrm{Cay}(R,S))$ *contains a subgroup $H$ with the following properties:*

- $A \leq H$,
- *the $A$-orbits are $H$-invariant, and*
- $|H : A|$ *does not divide* 4.

*Proof.* Let $\iota'$ be the automorphism of $A$ mapping every element to its inverse and let $A' = A \rtimes \langle \iota' \rangle$.

Suppose first that $\mathrm{Aut}(\mathrm{Cay}(A, A \cap S)) > A'$. By [3, Proof of Theorem 1.5], there are at most $2^{m/2+11n/48+2(\log_2(n))^2+2} = 2^{m/2+11n/48+o(n)}$ possible choices for $A \cap S$ with this property. Since $S$ is inverse-closed and no element of $R \setminus A$ is an involution, there are at most $2^{n/4}$ choices for $(R \setminus A) \cap S$. Thus altogether there are at most $2^{m/2+23n/48+o(n)}$ possible choices for $S$ in this case.

We now consider the case when $\mathrm{Aut}(\mathrm{Cay}(A, A \cap S)) = A'$. Let $H_A$ be the stabiliser in $H$ of the $A$-orbit $A$ and let $\Lambda$ be the group induced by the action of $H_A$ on $A$. Since $A \leq H_A$ and since $H$ acts as a group of automorphisms of $\mathrm{Cay}(R,S)$, we have $A \leq \Lambda \leq \mathrm{Aut}(\mathrm{Cay}(A, A \cap S)) = A'$.

From the Embedding Theorem [12, Theorem 1.2.6], $H \leq \Lambda \operatorname{wr} \mathrm{C}_2 = (\Lambda \times \Lambda) \rtimes \mathrm{C}_2$. (The first coordinate corresponds to the action on $A$ while the second coordinate corresponds to the action on $xA$.) Moreover, under this embedding, the group $A$ is identified with the diagonal subgroup $\{(z,z) \mid z \in A\}$ and $H_A \leq \Lambda \times \Lambda$. Let $K = \{(z_1, z_2) \in H_A \mid z_1 = 1\}$ and let $L = \{(z_1, z_2) \in H_A \mid z_1 \in \{1, \iota'\}\}$.

We claim that there exists $z = (z_1, z_2) \in L$ with $z_2 \notin \{1, y\}$. Assume, on the contrary, that $z_2 \in \{1, y\}$ for every $(z_1, z_2) \in L$. In particular, $|K| \leq 2$.

On the other hand, we have

$$|H : A| = |H : H_A||H_A : A| = |H : H_A||\Lambda : A||K|.$$

Since $A$ has two orbits which are $H$-invariant, we have $|H : H_A| \leq 2$. As $|H : A|$ does not divide 4 and $|\Lambda : A| \leq 2$, it follows that $|H : H_A| = |\Lambda : A| = |K| = 2$. We may thus assume that $K = \langle (1, y)\rangle$, that $H$ is transitive, and that $\Lambda = A'$.

Since $\Lambda = A'$, it follows that $|L| = 2|K| = 4$. As we are assuming that every element in $L$ has second coordinate in $\{1, y\}$, we get $L = \langle (1, y), (\iota', 1)\rangle$. Since $H$ is transitive, there exists $h \in H$ interchanging the two $A$-orbits. As the first coordinate of $(\iota', 1)^h$ is the identity, we get $(\iota', 1)^h \in K$ and hence $(\iota', 1)^h = (1, y)$. Observe that $\iota'$ fixes some but not all of the points of $A$, thus $(\iota', 1)^h = (1, y)$ fixes some but not all of the points of $xA$. This is a contradiction since $y$ acts fixed point-freely on $xA$. This completes the proof of our claim.

There are at most $2|A'| \leq 2^{o(n)}$ choices for $z$. We now assume that $z = (z_1, z_2)$ is fixed and count the number of elements $ax \in R \setminus A$ such that $(ax)^z \in \{ax, (ax)^{-1}\} = \{ax, axy\}$. First, suppose that $z_2 \in A$. In this case, we have $(ax)^z = axz_2$ and $axz_2 \in \{ax, axy\}$ if and only if $z_2 \in \{1, y\}$, which is a contradiction. Next, suppose that $z_2 = b\iota'$ for some $b \in A$. We have $(ax)^z = (axb)^{\iota'} = (ab^{-1}x)^{\iota'} = a^{-1}bx$ and $a^{-1}bx \in \{ax, axy\}$ if and only if $a^2 \in \{b, by\}$. By Lemma 2.3(1), the number of such $a$ is at most $2|A|/3$. In particular, there are at least $|A|/3 = n/6$ elements $a \in A$ such that $(ax)^z \notin \{ax, (ax)^{-1}\}$.

Since $z_1 \in \{1, \iota'\}$, it follows that $z$ fixes the vertex of $\mathrm{Cay}(R, S)$ corresponding to the identity and thus $S$ is $\langle z\rangle$-invariant. As $z \in H_A$, in fact $(R \setminus A) \cap S$ is $\langle z\rangle$-invariant and hence clearly $\langle z, \iota\rangle$-invariant as well. Since $R \setminus A$ does not contain any involutions, any element of $R \setminus A$ is in an orbit of length at least 2 under $\langle z, \iota\rangle$. Furthermore, observe that if $(ax)^z \notin \{ax, (ax)^{-1}\}$, then $ax$ is in an orbit of length at least 4 under $\langle z, \iota\rangle$. It follows that the number of choices for $(R \setminus A) \cap S$ is at most $2^{\frac{n/6}{4}+\frac{n/2-n/6}{2}} = 2^{5n/24}$. As the number of choices for $A \cap S$ is at most $2^{m/2+n/4}$, there are at most $2^{m/2+11n/24+o(n)}$ choices for $S$ in this case.

Adding the results we obtained in the two cases, we find that the number of choices for $S$ is at most $2^{m/2+23n/48+o(n)}$. □

Finally, we will need the following result. As the proof is long, technical, and different in flavour from the rest of the paper, we will present it separately in Section 6.

**Theorem 3.4.** *Assume Notation* 3.1. *Let $X = B/N$ be a quotient of $B$ and let $G$ be a primitive permutation group with point-stabiliser $X$. Then $G$ has a unique minimal normal subgroup. Moreover, either $G$ is of affine type or $y \in N$.*

We are now ready to prove the main theorem of this section.

**Theorem 3.5.** *Assume Notation* 3.1. *The number of inverse-closed subsets* $S$ *of* $R$ *such that* $\mathrm{Aut}(\mathrm{Cay}(R,S)) > B$ *is at most* $2^{m/2+23n/48+o(n)}$. *In particular, the proportion of inverse-closed subsets* $S$ *of* $R$ *such that* $\mathrm{Aut}(\mathrm{Cay}(R,S)) = B$ *goes to* 1 *as* $n \to \infty$.

*Proof.* Note that the number of inverse-closed subsets of $R$ is $2^{m/2+n/2}$, hence the second part of the theorem follows from the first. Let $S$ be an inverse-closed subset of $R$ such that $\mathrm{Aut}(\mathrm{Cay}(R,S)) > B$ and let $G$ be a subgroup of $\mathrm{Aut}(\mathrm{Cay}(R,S))$ containing $B$ as a maximal subgroup.

**Case 1.** $y$ is central in $G$.

Let $T = \{s \in S \mid sy \notin S\}$ and let $U = \langle T\rangle$. Since $S$ is $G_1$-invariant and $y$ is central in $G$, it follows that $T$ is $G_1$-invariant. Hence the $U$-orbits are $G_1$-invariant. Note that $\iota \in G_1$ and, for every $z \in R\setminus A$, we have $z^\iota = zy$. Since $S$ is $G_1$-invariant, this shows that $T \cap (R \setminus A) = \emptyset$, and hence $T \subseteq A$ and $U \leq A$. By Lemma 3.2(2), $R$ normalises every subgroup of $A$. In particular $R$ normalises $U$ and thus the $U$-orbits are invariant under $G = RG_1$.

Suppose first that $U = A$. Since $|B : A| = 4$ and $G > B$ we have $|G : A| > 4$. Therefore Lemma 3.3 (applied with $H = G$) implies that there are at most $2^{m/2+23n/48+o(n)}$ choices for $S$ in this case.

We now assume that $U < A$. By Lemma 2.8, there are at most $2^{o(n)}$ choices for $U$. Assume that $U$ is fixed and let $g$ be the permutation of $R$ that fixes every element of $U$ and every element of $R\setminus A$ but interchanges $a$ with $ay$ for every $a \in A\setminus U$. A few calculations reveal that $g$ is an automorphism of $\mathrm{Cay}(R,S)$ fixing the identity. Let $X = \{r \in R \mid \{r, r^{-1}\}^g \neq \{r, r^{-1}\}\}$ and note that, if $r \in A\setminus U$ and $r^2 \neq y$ then $r \in X$. Since $U < A$, it follows from Lemma 2.3(2) that $|X| \geq |A|/4$. Let $m_1$ be the number of involutions in $X$. Note that $X$ is itself inverse-closed. The number of inverse-closed subsets of $R \setminus X$ is exactly

$$2^{(m-m_1)+((n-|X|)-(m-m_1))/2} = 2^{(m-m_1)/2+(n-|X|)/2}$$

and hence this is an upper bound for the number of choices for $(R\setminus X) \cap S$.

Involutions of $R$ lying in $X$ are in $\langle g\rangle$-orbits of length at least 2; while if $x$ is a non-involution in $X$, then $\{x, x^{-1}\}^g \neq \{x, x^{-1}\}$ and hence the smallest $\langle g\rangle$-invariant inverse-closed subset of $X$ containing $x$ has size at least 4. Since $S$ is inverse-closed and $\langle g\rangle$-invariant, the number of choices for $X \cap S$ is at most $2^{m_1/2+(|X|-m_1)/4}$. Hence the total number of choices for $S$ is at most $2^{m/2+n/2-|X|/4-m_1/4} \leq 2^{m/2+n/2-|X|/4}$. Since $|X| \geq |A|/4$, it follows that there are at most $2^{m/2+15n/32+o(n)}$ choices for $S$ in this case.

**Case 2.** $y$ is not central in $G$.

Let $N$ be the core of $B$ in $G$, that is $N = \bigcap_{g\in G} B^g$. We will use the "bar convention" and, for all $X \leq G$, denote the group $XN/N$ by $\overline{X}$. It follows from Lemma 2.2(2) and Lemma 3.2(6) that $\langle y\rangle$ is characteristic in $B$. Since $y$ is not central in $G$, $B$ is not normal in $G$ and thus $N < B$. As

$B$ is maximal in $G$, we have that $\overline{G}$ is a primitive permutation group on the cosets of $\overline{B}$, with point-stabiliser $\overline{B}$.

Suppose that $N \not\leq C$. Fix $cx \in N \cap (B \setminus C)$ where $c \in C$. For every $a \in A$ we have $(cx)^a = cx^a = cxa^2 \in N$ thus $a^2 \in N$ and hence $A^2 \leq N$. Moreover $(cx)(cx)^x = cxx^{-1}cxx = c^2y \in N$. Since $C^2 = A^2 \leq N$, this shows that $y \in N$ and hence $\langle A^2, y\rangle \leq N$. This implies that $\overline{B}$ is an elementary abelian 2-group. By Lemmas 2.4 and 2.5, it follows that $\overline{B}$ is cyclic of order 2. Since the point-stabiliser of a primitive group is self-normalising, $\overline{B}$ is a Sylow 2-subgroup of $\overline{G}$ and $|G : B|$ is odd.

Suppose that $N \neq D$. Since $|B : N| = 2$, it follows by Lemma 3.2(7) that $y \in N$ and the orbit of $y$ under $\mathrm{Aut}(N)$ has size at most 2. Since $|G : B|$ is odd and $y$ is central in $B$, this implies that $y$ is central in $G$, which is a contradiction.

We may thus assume that $N = D$. Since $A$ is characteristic in $D$, it follows that $A$ is normal in $G$. By Lemma 3.3 (applied with $H = G$), there are at most $2^{m/2+23n/48+o(n)}$ choices for $S$ in this case.

From now on, we assume that $N \leq C$. By Theorem 3.4, $\overline{G}$ has a unique minimal normal subgroup $T/N$.

Suppose that $N < C$ and that $y \in N$. Since $C$ is abelian, we have $N < C \leq \mathbf{C}_G(N) \trianglelefteq G$ and thus $1 < \overline{\mathbf{C}_G(N)} \trianglelefteq \overline{G}$. As $T/N$ is the unique minimal normal subgroup of $\overline{G}$, it follows that $T \leq \mathbf{C}_G(N)$. In particular, $y$ is centralised by $T$. As $y$ is central in $B$, $y$ is central in $BT = G$, which is a contradiction.

We may thus assume that either $N = C$ or $y \notin N$. If $N = C$ then $|\overline{B}| = 2$ and thus $\overline{G}$ is dihedral and $\overline{T}$ is odd. If $y \notin N$ then, by Theorem 3.4, $\overline{G}$ is of affine type. Since $y \notin N$, it follows that the centre of $\overline{B}$ has even order and thus, by Lemma 2.5, $|\overline{T}|$ is odd.

In both cases, we have obtained that $\overline{G}$ is of affine type and $|\overline{T}|$ is odd. It follows that $|T : N| = |CT : C|$ is odd. Since $C$ has two orbits, namely $A$ and $R \setminus A$, and these have the same size, $CT$ is intransitive with the same orbits as $C$. As $|G : CT| = |B : C| = 2$, $CT$ is normal in $G$ and it follows from Lemma 3.3 (applied with $H = CT$) that there are at most $2^{m/2+23n/48+o(n)}$ choices for $S$ in this case.

Adding the results we obtained in the four cases, we find that the number of choices for $S$ is at most $2^{m/2+23n/48+o(n)}$. □

## 4. Cayley graphs on $\mathrm{Q}_8 \times \mathrm{C}_2^\ell$

Before stating the main result of this section, we need to introduce some notation.

**Notation 4.1.** Let $E$ be an elementary abelian 2-group, let $\mathrm{Q}_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, i^j = i^{-1}\rangle$ and let $R = \mathrm{Q}_8 \times E$. We label the elements of $\mathrm{Q}_8$ with $\{1, -1, i, -i, j, -j, k, -k\}$ in the usual way. Let $M = \langle -1\rangle \times E$, let $n = |R|$ and let $m$ be the number of elements of order at most 2 in $R$. We define the following permutations of $R$: for $\ell \in \{i, j, k\}$, $\alpha_\ell$ is the involution that swaps $\ell e$ and$-\ell e$ for every $e \in E$ and fixes every other element of $R$. Let $B = \langle R, \alpha_i, \alpha_j, \alpha_k \rangle$, viewed as a permutation group on $R$ (with $R$ acting regularly on itself by right multiplication).

The importance of $B$ in this context can be seen with the following observation.

**Lemma 4.2.** *Assume Notation* 4.1. *Every Cayley graph on* $R$ *admits* $B$ *as a group of automorphisms.*

*Proof.* Let $S$ be an inverse-closed subset of $R$, let $x, y \in R$, let $s = xy^{-1}$ and write $x = qe$ and $y = rf$ with $q, r \in \mathrm{Q}_8$ and $e, f \in E$. Note that

$$x^{\alpha_i}(y^{\alpha_i})^{-1} = \begin{cases} -s & \text{if } |\{q,r\} \cap \{i,-i\}| = 1, \\ s & \text{otherwise.} \end{cases}$$

Moreover, if $|\{q,r\} \cap \{i,-i\}| = 1$ then $-s = s^{-1}$ and thus $x^{\alpha_i}(y^{\alpha_i})^{-1} \in \{s, s^{-1}\}$ in all cases. This implies that $\alpha_i$ is an automorphism of $\mathrm{Cay}(R,S)$. By an analogous argument, the same is true for $\alpha_j$ and $\alpha_k$ and the result follows. □

The main result of this section is that almost all Cayley graphs on $R$ have $B$ as their full automorphism group. Before we state and prove this, we collect a few basic results about $B$ which will be used repeatedly. The proofs are left to the reader.

**Lemma 4.3.** *Assume Notation* 4.1. *Then*

1. $M = \mathbf{Z}(B)$,
2. $|B : R| = 8$,
3. *$B$ has exponent* 4,
4. $m = |M| = n/4$, *and*
5. *$R$ has exactly* $2^{5n/8}$ *inverse-closed subsets.*

**Theorem 4.4.** *Assume Notation* 4.1. *The number of inverse-closed subsets $S$ of $R$ such that* $\mathrm{Aut}(\mathrm{Cay}(R,S)) > B$ *is at most* $2^{5n/8 - n/512 + o(n)}$. *In particular, the proportion of inverse-closed subsets $S$ of $R$ such that* $\mathrm{Aut}(\mathrm{Cay}(R,S)) = B$ *goes to* 1 *as* $n \to \infty$.

*Proof.* By Lemma 4.3(5), the number of inverse-closed subsets of $R$ is $2^{5n/8}$, hence the second part of the theorem follows from the first.

Let $S$ be an inverse-closed subset of $R$ such that $\mathrm{Aut}(\mathrm{Cay}(R,S)) > B$, let $G$ be a subgroup of $\mathrm{Aut}(\mathrm{Cay}(R,S))$ containing $B$ as a maximal subgroup and let $g \in G_1 \setminus B_1$. As $B$ is maximal in $G$, we have $G = \langle B, g \rangle$.

**Case 1.** $M$ is normal in $G$.

Suppose that $M$ is not centralised by $G_1$. In particular, there is some element of $G_1$ the action of which by conjugation on $M$ induces a non-trivial automorphism $\phi$ of $M$. Since $\phi$ fixes at most half of the elements of $M$, the number of subsets of $M$ which are $\phi$-invariant is at most $2^{|M|/2}2^{|M|/4} = 2^{3|M|/4} = 2^{3n/16}$. By Lemma 2.8, there are at most $2^{o(n)}$ choices for $\phi$ and thus at most $2^{3n/16+o(n)}$ choices for $M \cap S$. Since all of the involutions of $R$ are in $M$, the number of inverse-closed subsets of $R \backslash M$ is $2^{(n-|M|)/2} = 2^{3n/8}$. This is an upper bound for the number of choices for $(R \backslash M) \cap S$. The number of choices for $S$ is thus at most $2^{9n/16+o(n)}$ in this case.

We now assume that $M$ is centralised by $G_1$. Suppose that $G_1$ is not contained in the kernel of the action of $G$ on $M$-orbits. By Lemma 2.9 there are at most $2^{m/2+n/2-|M|/2+o(n)} = 2^{n/2+o(n)}$ choices for $S$ in this case.

We now assume that $G_1$ fixes every $M$-orbit setwise. In what follows, for $r \in R$ and $h \in G$, we write $r^h$ to denote the image of the vertex $r$ under the permutation $h$, and $h^{-1}rh$ to denote the conjugate of the permutation $r \in G$ by the element $h$. Let $i^g = iq_i$, $j^g = jq_j$ and $k^g = kq_k$, where $q_i, q_j, q_k \in M$. Since $g$ centralises $M$, we have $(\ell m)^g = \ell^g m = \ell q_\ell m$ for every $m \in M$ and every $\ell \in \{i, j, k\}$. It follows that $g$ is determined by $q_i$, $q_j$ and $q_k$ and thus there are at most $|M|^3 \leq 2^{o(n)}$ choices for $g$.

Suppose that $q_i, q_j, q_k \in \{-1, 1\}$. Note that $\alpha_i, \alpha_j \in B_1$. By replacing $g$ by an element of $\{g, g\alpha_i, g\alpha_j, g\alpha_i\alpha_j\}$, we may assume that $q_i = q_j = 1$. Since $g \neq 1$, we have $q_k = -1$ and hence $g = \alpha_k$, contradicting the fact that $g \notin B_1$.

We may thus assume that $q_{\bar{\ell}} \notin \{-1, 1\}$ for some $\bar{\ell} \in \{i, j, k\}$. It follows that, for every $m \in M$, we have $(\bar{\ell}m)^g \notin \{\bar{\ell}m, (\bar{\ell}m)^{-1}\}$. Since $\bar{\ell}M \cap S$ is inverse-closed and preserved by $g$, there are at most $2^{|\bar{\ell}M|/4} = 2^{n/16}$ choices for $\bar{\ell}M \cap S$. As the number of choices for $M \cap S$ is at most $2^{n/4}$ and the number of choices for $\ell M \cap S$ is at most $2^{n/8}$ for each $\ell \in \{i, j, k\} \setminus \{\bar{\ell}\}$, there are at most $2^{9n/16+o(n)}$ choices for $S$ in this case.

**Case 2.** *$M$ is not normal in $G$.*

Since $M = \mathbf{Z}(B)$, $B$ is not normal in $G$ either. Since $B$ is maximal but not normal in $G$, it must be self-normalising in $G$ and thus $\langle B, B^g \rangle = G$. Moreover, since $B$ is a 2-group, it follows that $B$ must be a Sylow 2-subgroup of $G$ and hence $|G : B|$ is odd. In particular, by the orbit-stabiliser theorem, $G_1$ is not a 2-group.

Let $H = M \cap M^g$. Since $M = \mathbf{Z}(B)$, $H$ is central in $B$. By the same reasoning, $H$ is central in $B^g$ and thus in $\langle B, B^g \rangle = G$.

Let $N$ be the core of $B$ in $G$. Note that $H \leq N < B$ and, since $B$ is maximal in $G$, we can view $G/N$ as a primitive permutation group with point-stabiliser $B/N$. As $B$ has exponent 4, $B/N$ has exponent dividing 4 and hence, by Corollary 2.7, $G/N$ is of affine type. Moreover, since $MN/N$ is contained in the centre of $B/N$, it follows from Lemma 2.5 that $MN/N$ is cyclic. Since $M$ is an elementary abelian 2-group, so is $MN/N$ and hence $|MN : N| \leq 2$.

As $|B : M| = 32$, we have $|MN : M| \leq 32$. It follows that $|N : N \cap M| \leq 32$ and hence $|N \cap M^g : N \cap M \cap M^g| = |N \cap M^g : H| \leq 32$. Applying $g^{-1}$ to $N \cap M^g$ and $H$, we obtain $|N \cap M : H| \leq 32$. As $|MN : N| \leq 2$, we have $|M : N \cap M| \leq 2$ and hence $|M : H| = |M : N \cap M||N \cap M : H| \leq 2 \cdot 32 = 64$. Finally, $|R : M| = 4$ and hence $|R : H| \leq 256$.

Suppose that $G_1$ is contained in the kernel of the action of $G$ on $H$-orbits. It follows that $HG_1$ is normal in $G$. Since $H$ is central in $G$ and $H \cap G_1 = 1$, we have $HG_1 = H \times G_1$. As $HG_1$ is normal in $G$, we have $\langle z^2 \mid z \in HG_1\rangle = \langle z^2 \mid z \in G_1\rangle$ is normal in $G$ and hence $\langle z^2 \mid z \in G_1\rangle = 1$ because $G_1$ is core-free in $G$. Thus $G_1$ is an elementary abelian 2-group, which is a contradiction.

We may thus assume that $G_1$ is not contained in the kernel of the action of $G$ on $H$-orbits. It then follows from Lemma 2.9 that there are at most $2^{m/2+n/2-|H|/2+o(n)} = 2^{5n/8-n/512+o(n)}$ choices for $S$ in this case.

Adding the results we obtained in the four cases, we find that the number of choices for $S$ is at most $2^{5n/8-n/512+o(n)}$. □

Combined together, Theorems 3.5 and 4.4 yield Theorem 1.4.

## 5. Related results: Unlabelled graphs, and digraphs

An *unlabelled* graph is simply an isomorphism class of (labelled) graphs. We often identify a representative with its class. An easy consequence of Theorems 3.5 and 4.4 is the following unlabelled version of Theorem 1.4.

**Theorem 5.1.** *Let $R$ be a generalised dicyclic group of order $n$, $B = R \rtimes \langle \iota \rangle$ if $R \not\cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ and let $B$ be as in Notation 4.1 if $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$. The proportion of unlabelled Cayley graphs $\Gamma$ over $R$ such that $\mathrm{Aut}(\Gamma) = B$ goes to 1 as $n \to \infty$.*

*Proof.* Let $\Gamma_1 = \mathrm{Cay}(R, S_1)$ with $\mathrm{Aut}(\Gamma_1) = B$. We show that the number of inverse-closed subsets $S_2$ of $R$ such that $\Gamma_1 \cong \mathrm{Cay}(R, S_2)$ is at most $2^{o(n)}$. The result then follows from Theorems 3.5 and 4.4.

Let $\Gamma_2 = \mathrm{Cay}(R, S_2)$ and let $\varphi$ be a graph isomorphism from $\Gamma_1$ to $\Gamma_2$. Note that $\varphi$ induces a group isomorphism, $\phi$ say, from $\mathrm{Aut}(\Gamma_1) = B$ to $\mathrm{Aut}(\Gamma_2) = B$ and hence $\phi \in \mathrm{Aut}(B)$.

Note that there exists a characteristic subgroup $X$ of $B$ such that $X \leq R$ and $|B : X| \leq 32$. (If $R \not\cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ then take $X = R$ and use Lemma 3.2(6), if $R \cong \mathrm{Q}_8 \times \mathrm{C}_2^\ell$ then take $X = M$ as in Notation 4.1.) It follows that $X \leq R^\phi$. Since $|B : X| \leq 32$, it follows that $B$ has at most $O(1)$ subgroups containing $X$ and thus there are at most $O(1)$ choices for the subgroup $R^\phi$. As $|\mathrm{Aut}(R)| \leq 2^{o(n)}$, there are at most $2^{o(n)}$ choices for an isomorphism from $R$ to a given $R^\phi$ and thus at most $2^{o(n)}$ choices for $\phi$ (and hence for $\varphi$ and $S_2$). □

One can define *Cayley digraphs* in the obvious way: if $S$ is a (not necessarily inverse-closed) subset of a group $R$ then $\mathrm{Cay}(R, S)$ is the digraph with vertex-set $R$ and with $(g, h)$ being an arc if and only if $gh^{-1} \in S$. Our proof of Theorem 1.4 with a few minor adjustments yields the corresponding directed version.

**Theorem 5.2.** *Let $R$ be a generalised dicyclic group of order $n$. The proportion of subsets $S$ of $R$ such that $\mathrm{Aut}(\mathrm{Cay}(R, S)) = R$ goes to 1 as $n \to \infty$.*

## 6. Proof of Theorem 3.4

This section is dedicated solely to the proof of Theorem 3.4. We first need a few preliminary results.

**Lemma 6.1.** *A primitive permutation group with generalised dicyclic point-stabilisers is of affine type.*

*Proof.* Let $R = \mathrm{Dic}(A, y, x)$ be a point-stabiliser of the primitive group $G$. Suppose first that $R \cap R^g = 1$ for every $g \in G \setminus R$. Then, $G$ is a Frobenius group with complement $R$. Since $G$ is primitive, the Frobenius kernel is an elementary abelian group and $G$ is of affine type. We may thus assume that there exists $\bar{g} \in G \setminus R$ with $R \cap R^{\bar{g}} \neq 1$.

Since $R$ is a maximal subgroup of $G$, $R$ is self-normalising in $G$. It follows that $R^{\bar{g}} \neq R$ and hence $\langle R, R^{\bar{g}} \rangle = G$. Since every subgroup of $A$ is normal in $R$, $A \cap A^{\bar{g}} \trianglelefteq R$. For the same reason, $A \cap A^{\bar{g}} \trianglelefteq R^g$ and thus $A \cap A^{\bar{g}} \trianglelefteq G$. Since $A \cap A^{\bar{g}}$ is contained in the point-stabiliser $R$, it follows that $A \cap A^{\bar{g}} = 1$.

In particular, we have either $R \cap R^{\bar{g}} \nleq A$ or $R \cap R^{\bar{g}} \nleq A^{\bar{g}}$. By symmetry, we may assume that the former holds. As $|R : A| = 2$, we get $R = A(R \cap R^{\bar{g}})$ hence $ax \in R \cap R^{\bar{g}}$ for some $a \in A$. The square of every element of $R^{\bar{g}}$ lies in $A^{\bar{g}}$ thus $(ax)^2 = y \in A^{\bar{g}}$. Since $y \in A$, this contradicts the fact that $A \cap A^{\bar{g}} = 1$. □

**Lemma 6.2.** *Assume Notation* 3.1. *A primitive permutation group with point-stabiliser $B$ is of affine type.*

*Proof.* Let $G$ be a primitive group with point-stabiliser $B$ and, towards a contradiction, suppose that $G$ is not of affine type.

Suppose that $x \in B \cap B^g$ for some $g \in G \setminus B$. Since the square of an element of order 4 in $B$ in necessarily central in $B$, $x^2$ is central in $B$. A similar reasoning implies that $x^2$ is central in $B^g$ and thus in $\langle B, B^g \rangle = G$. Since $B$ is core-free in $G$ and $1 \neq x^2 = y \in B$, we reach a contradiction.

It follows that for every $g \in G \setminus B$, $x \notin B \cap B^g$. In particular, $x$ fixes only one point. Since $x$ has order 4, this implies that $G$ has odd degree. It then follows from [10, Theorem] that $G$ is either of almost simple or of product action type. In particular, $G$ has a unique minimal normal subgroup $N$.

**Case 1.** $G$ is of almost simple type.

In this case, the structure of $N$ and $B \cap N$ are described in [10, Theorem, Part (b)]. In order to use this classification more effectively, we first make some observations about $B \cap N$.

It follows from [11, Theorem 1] that $\mathbf{Z}(B)$ is cyclic. Since all elements of order at most 2 in $A$ are central in $B$, it follows that $y$ is the unique involution in $A$ and the Sylow 2-subgroup of $A$ is cyclic. Let $a$ be a generator of the Sylow 2-subgroup of $A$, let $2^\ell$ be the order of $a$ and let $B_2 = \langle a, x, \iota \rangle$. Clearly, $B_2$ is a Sylow 2-subgroup of $B$, and hence of $G$. Thus $B_2 \cap N$ is a Sylow 2-subgroup of $N$.

Suppose that $B_2 \cap N \leq R = \langle A, x \rangle$, that is, $B_2 \cap N \leq \langle a, x \rangle$. Observe that $\langle a, x \rangle$ is a generalised quaternion group. Thus $B_2 \cap N$ is either cyclic or a generalised quaternion group. By [2], a non-abelian simple group cannot have a cyclic or generalised quaternion group Sylow 2-subgroup, which is a contradiction.

Suppose that $B_2 \cap N \leq C = A \times \langle \iota \rangle$, that is, $B_2 \cap N \leq \langle a \rangle \times \langle \iota \rangle$. Then $N$ has an abelian Sylow 2-subgroup and hence, by the remarkable theorem of Walter [14], $N$ is isomorphic either to $\mathrm{PSL}(2, 2^f)$ for some $f \geq 3$, to $\mathrm{PSL}(2, q)$ for some $q \equiv 3, 5 \pmod 8$, to the Janko group $J_1$, or to a Ree group $\mathrm{Ree}(3^{2m+1})$ for some $m \geq 1$. Since $B_2 \cap N$ is 2-generated, a quick inspection reveals that $N \cong \mathrm{PSL}(2, q)$ for some $q \equiv 3, 5 \pmod 8$. In particular, $|B_2 \cap N| = 4$ and hence $B_2 \cap N = \langle y \rangle \times \langle \iota \rangle$. As $q \equiv 3, 5 \pmod 8$, $q$ is not a square and hence $\mathrm{Out}(N) \cong \mathrm{Out}(\mathrm{PSL}(2, q))$ is cyclic of odd order. Since $G/N$ is isomorphic to a subgroup of $\mathrm{Out}(N)$, so is $B_2N/N \cong B_2/(B_2 \cap N)$ and hence $B_2 \leq N$. This is a contradiction since $B_2$ has order at least 8 while $B_2 \cap N$ has order 4.

We conclude that $B_2 \cap N \leq \langle a, \iota, x \rangle$ but $B_2 \cap N \nleq \langle a, \iota \rangle$ and $B_2 \cap N \nleq \langle a, x \rangle$. Combining this information with the description of the primitive almost simple groups of odd degree in [10, Theorem, Part (b)] and the classification of the maximal solvable subgroups of almost simple groups in [8] yields that $N \cong \mathrm{PSL}(2, q)$, and either $B \cap N \cong \mathrm{D}_{(q+1)/2}$ and $q \equiv 3 \pmod 4$, or $B \cap N \cong \mathrm{D}_{(q-1)/2}$ and $q \equiv 1 \pmod 4$.

If $q \in \{5, 7, 9\}$ then the conclusion follows by computation (no group $G$ with $N \leq G \leq \mathrm{P\Gamma L}(2, q)$ has a Sylow 2-subgroup isomorphic to a Sylow 2-subgroup of $B$). We thus assume that $q \geq 11$ and write $\varepsilon = 1$ if $q \equiv 1 \pmod 4$ and $\varepsilon = -1$ if $q \equiv 3 \pmod 4$. Since $A \times \langle \iota \rangle$ is an abelian subgroup of index 2 in $B$, $(A \times \langle \iota \rangle) \cap N$ is an abelian subgroup of index at most 2 in $B \cap N = \mathrm{D}_{(q-\varepsilon)/2}$. Let $A_0 = (A \times \langle \iota \rangle) \cap N$. As $q - \varepsilon \geq 10$, $\mathrm{D}_{(q-\varepsilon)/2}$ has a unique abelian subgroup of index at most 2 and hence $A_0 \cong \mathrm{C}_{(q-\varepsilon)/2}$ and, in particular, $A_0$ is a maximal torus of $N$. After two computations, one for the case $\varepsilon = 1$ and one of the case $\varepsilon = -1$, we see that $\mathbf{C}_{\mathrm{P\Gamma L}(2,q)}(A_0) \leq \mathrm{PGL}(2, q)$, and hence $A \times \langle \iota \rangle \leq \mathrm{PGL}(2, q)$. Since $\mathbf{C}_{\mathrm{P\Gamma L}(2,q)}(A_0) = \mathbf{C}_{\mathrm{PGL}(2,q)}(A_0)$ is a maximal torus of $\mathrm{PGL}(2, q)$ of order $q - \varepsilon$, we obtain that $A \times \langle \iota \rangle$ is cyclic. This implies that $A$ has odd order, which is a contradiction.

**Case 2.** *$G$ is of product action type.*

In particular, $N \trianglelefteq G \leq H \operatorname{wr} \mathrm{Sym}(\ell)$ with $\ell \geq 2$, $H$ an almost simple group with socle $T$ and with $N \cong T^\ell$. Let $N = T_1 \times \cdots \times T_\ell$ with $T_i \cong T$ for every $i \in \{1, \ldots, \ell\}$.

For every $i \in \{1, \ldots, \ell\}$, let $B_i = B \cap T_i$. From the structure of primitive permutation groups of product action type [9], we have $B \cap N = B_1 \times \cdots \times B_\ell$ with $|B_1| = \cdots = |B_\ell| > 1$. As $N$ is transitive, we have $G = NB$. It follows that $B$ acts transitively by conjugation on the set $\{T_1, \ldots, T_\ell\}$ and thus on $\{B_1, \ldots, B_\ell\}$ and, since $R \trianglelefteq B$, also on $\{(B_1 \cap R), \ldots, (B_\ell \cap R)\}$. In particular, the groups $B_1 \cap R, \ldots, B_\ell \cap R$ are pairwise conjugate in $B$ and pairwise intersect trivially. Since $\ell \geq 2$, it follows from Lemma 3.2(5) that $B_1 \cap R = \cdots = B_\ell \cap R = 1$. As $|B : R| = 2$, we have $|B_i| = 2$ for every

$i \in \{1, \dots, \ell\}$ and hence $B \cap N = B_1 \times \cdots \times B_\ell$ is an elementary abelian 2-group.

Since $B = \mathbf{N}_G(B \cap N)$, it follows that $B \cap N = \mathbf{N}_N(B \cap N)$ and $B_i = \mathbf{N}_{T_i}(B_i)$ for every $i \in \{1, \dots, \ell\}$. Since $B_i$ has order 2 and is self-normalising in $T_i$, it must be a Sylow 2-subgroup of $T_i$. This is a contradiction since a non-abelian simple group cannot have a Sylow 2-subgroup of order 2 (see [7, 7.2.1] for example). □

We now prove Theorem 3.4 which we restate, for convenience.

**Theorem 3.4.** *Assume Notation* 3.1. *Let $X = B/N$ be a quotient of $B$ and let $G$ be a primitive permutation group with point-stabiliser $X$. Then $G$ has a unique minimal normal subgroup. Moreover, either $G$ is of affine type or $y \in N$.*

*Proof.* Observe that $X$ is solvable. The finite primitive permutation groups with solvable point-stabilisers are classified in [8]. From [8, Theorem 1.1] we see that $G$ is either of affine, almost simple or product action type. In particular, $G$ has a unique minimal normal subgroup. Suppose that $y \notin N$. We show that $G$ is of affine type.

By Lemma 2.4 we may assume that $X$ is non-abelian. If $N \not\leq C$ then $B = NC$ and $X = B/N \cong C/(C \cap N)$ is abelian, which is a contradiction. We may thus assume that $N \leq C$.

If $N \not\leq R$ then $B = NR$ and $X = B/N \cong R/(R \cap N)$. Since $X$ is non-abelian and $y \notin N$, it follows that $X$ is a generalised dicyclic group and hence $G$ is of affine type by Lemma 6.1. We may thus assume that $N \leq R$ and hence $N \leq C \cap R = A$.

As $y \notin N$, we obtain that $R/N$ is isomorphic to the generalised dicyclic group $\mathrm{Dic}(A/N, yN, xN)$, $X = B/N$ is isomorphic to a group as in Notation 3.1 and hence $G$ is of affine type by Lemma 6.2. □

## References

[1] L. Babai, C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15.

[2] R. Brauer, M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, *Proc. Nat. Acad. Sci. U.S.A.* **45** (1959), 1757–1759.

[3] E. Dobson, P. Spiga, G. Verret, Cayley graphs on abelian groups, `arXiv:1306.3747v1`.

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory*, Vol. I, II (Szeged, 1978), pp. 221–239, Colloq. Math. Soc. János Bolyai, Amsterdam-New York, 1981.

[5] D. Hetzel, Über reguläre graphische Darstellungen von auflösbaren Gruppen, Technische Universität, Berlin, 1976. (Diplomarbeit)

[6] W. Imrich, Graphical regular representations of groups of odd order, *Combinatorics* (Proc. Colloq., Keszthely, 1976), Bolyai–North-Holland, 1978, 611–621.

[7] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups, An Introduction*, Universitext, Springer 2004.

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

[9] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Austral. Math. Soc. Ser. A* **44** (1988), 389–396.

[10] M. W. Liebeck, J. Saxl, The Primitive Permutation Groups of Odd Degree, *J. London Math. Soc.* **31** (1985), 250–264.

[11] M. W. Liebeck, J. Saxl, On Point Stabilizers in Primitive Permutation Groups, *Communications in Algebra* **19** (1991), 2777–2786.

[12] J. D. P. Meldrum, Wreath products of groups and semigroups, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 74, Longman, Harlow, 1995.

[13] L. A. Nowitz, M. E. Watkins, Graphical regular representations of non-abelian groups I-II, *Canad. J. Math.* **24** (1972), 993–1008 and 1009–1018.

[14] J. H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. Math.* **89** (1969), 405–514.

Joy Morris, Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB. T1K 3M4. Canada
*E-mail address*: `joy@cs.uleth.ca`

Pablo Spiga, Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca, Via Cozzi 53, 20125 Milano, Italy
*E-mail address*: `pablo.spiga@unimib.it`

Gabriel Verret, Centre for Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia.
Also affiliated with : UP FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia.
*E-mail address*: `gabriel.verret@uwa.edu.au`