DIGRAPHS WITH SMALL AUTOMORPHISM GROUPS THAT ARE CAYLEY ON TWO NONISOMORPHIC GROUPS

LUKE MORGAN, JOY MORRIS, AND GABRIEL VERRET

Abstract. Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph on a group G and let $A = \mathrm{Aut}(\Gamma)$. The *Cayley index* of Γ is $|A : G|$. It has previously been shown that, if p is a prime, G is a cyclic p-group and A contains a noncyclic regular subgroup, then the Cayley index of Γ is superexponential in p.

We present evidence suggesting that cyclic groups are exceptional in this respect. Specifically, we establish the contrasting result that, if p is an odd prime and G is abelian but not cyclic, and has order a power of p at least p^3, then there is a Cayley digraph Γ on G whose Cayley index is just p, and whose automorphism group contains a nonabelian regular subgroup.

1. Introduction

Every digraph and group in this paper is finite. A *digraph* Γ consists of a set of *vertices* $\mathrm{V}(\Gamma)$ and a set of *arcs* $\mathrm{A}(\Gamma)$, each arc being an ordered pair of distinct vertices. (Our digraphs do not have loops.) We say that Γ is a *graph* if, for every arc (u, v) of Γ, (v, u) is also an arc. Otherwise, Γ is a *proper* digraph.

The *automorphisms* of Γ are the permutations of $\mathrm{V}(\Gamma)$ that preserve $\mathrm{A}(\Gamma)$. They form a group under composition, denoted $\mathrm{Aut}(\Gamma)$.

Let G be a group and let S be a subset of G that does not contain the identity. The *Cayley digraph* on G with connection set S is $\Gamma = \mathrm{Cay}(G, S)$, the digraph with vertex-set G and where $(u, v) \in \mathrm{A}(\Gamma)$ whenever $vu^{-1} \in S$. The index of G in $\mathrm{Aut}(\Gamma)$ is called the *Cayley index* of Γ.

It is well-known that a digraph is a Cayley digraph on G if and only if its automorphism group contains the right regular representation of G. A digraph may have more than one regular subgroup in its automorphism group and hence more than one representation as a Cayley digraph. This is an interesting situation that has been studied in [3, 9, 12, 13, 15], for example.

Let p be a prime. Joseph [7] proved that if Γ has order p^2 and $\mathrm{Aut}(\Gamma)$ has two regular subgroups, one of which is cyclic and the other not, then Γ has Cayley index at least p^{p-1}. The second author generalised this in [11], showing that if $p \geqslant 3$, Γ has order p^n and

2010 *Mathematics Subject Classification.* 05C25, 20B25.

Key words and phrases. Cayley digraphs, Cayley index.

This research was supported by the Australian Research Council grant DE160100081 and by the Natural Science and Engineering Research Council of Canada. The first and last authors also thank the second author and the University of Lethbridge for hospitality.

$\mathrm{Aut}(\Gamma)$ has two regular subgroups, one of which is cyclic and the other not, then Γ has Cayley index at least $p^{p(n-1)-1}$. A simpler proof of this was later published in [1]. Kovács and Servatius [8] proved the analogous result when $p = 2$.

The theme of the results above is that if $\mathrm{Aut}(\Gamma)$ has two regular subgroups, one of which is cyclic and the other not, then Γ must have "large" Cayley index. (In fact, close examination of the proofs of the results above reveals that $\mathrm{Aut}(\Gamma)$ having two distinct regular subgroups, one of which is cyclic, might suffice. We will not dwell on this point.)

The goal of this paper is to show that cyclic p-groups are exceptional with respect to this property, at least among abelian p-groups. More precisely, we prove the following.

Theorem 1.1. *Let p be an odd prime and let G be an abelian p-group. If G has order at least p^3 and is not cyclic, then there exists a proper Cayley digraph on G with Cayley index p and whose automorphism group contains a nonabelian regular subgroup.*

It would be interesting to generalise Theorem 1.1 to nonabelian p-groups and to 2-groups. More generally, we expect that "most" groups admit a Cayley digraph of "small" Cayley index such that the automorphism group of the digraph contains another (or even a nonisomorphic) regular subgroup. At the moment, we do not know how to approach this problem in general, or even what a sensible definition of "small" might be. (Lemma 3.2 shows that the smallest index of a proper subgroup of either of the regular subgroups is a lower bound – and hence that the Cayley index of p in Theorem 1.1 is best possible.) As an example, we prove the following.

Proposition 1.2. *Let G be a group generated by an involution x and an element y of order 3, and such that $\mathbb{Z}_6 \ncong G \ncong \mathbb{Z}_3 \wr \mathbb{Z}_2$. If G has a subgroup H of index 2, then there is a Cayley digraph Γ with Cayley index 2 such that $\mathrm{Aut}(\Gamma)$ contains a regular subgroup distinct from G and isomorphic to $H \times \mathbb{Z}_2$.*

This paper is laid out as follows. Section 2 includes structural results on cartesian products of digraphs that will be required in the proofs of our main results, while in Section 3 we collect results about automorphism groups of digraphs. Section 4 consists of the proof of Theorem 1.1. Finally, in Section 5 we prove Proposition 1.2 and consider the case of symmetric groups.

2. Cartesian products

The main result of this section is a version of a result about cartesian products of graphs due to Imrich [6, Theorem 1] that is adapted to the case of proper digraphs. Imrich's proof can be generalised directly to all digraphs, but his proof involves a detailed case-by-case analysis for small graphs, which can be avoided by restricting attention to proper digraphs.

The *complement* of a digraph Γ, denoted $\overline{\Gamma}$, is the digraph with vertex-set $\mathrm{V}(\Gamma)$, with $(u, v) \in \mathrm{A}(\overline{\Gamma})$ if and only if $(u, v) \notin \mathrm{A}(\Gamma)$, for every two distinct vertices u and v of Γ. It is easy to see that a digraph and its complement have the same automorphism group.

Given digraphs Γ and Δ, the *cartesian product* $\Gamma \Box \Delta$ is the digraph with vertex-set $\mathrm{V}(\Gamma) \times \mathrm{V}(\Delta)$ and with $((u, v), (u', v'))$ being an arc if and only if either $u = u'$ and $(v, v') \in \mathrm{A}(\Delta)$, or $v = v'$ and $(u, u') \in \mathrm{A}(\Gamma)$. For each $u \in \mathrm{V}(\Gamma)$, we obtain a *copy* Δ^u of Δ in $\Gamma \Box \Delta$,

the induced digraph on $\{(u, v) \mid v \in \mathrm{V}(\Delta)\}$. Similarly, for each $v \in \mathrm{V}(\Delta)$, we obtain a copy Γ^v of Γ in $\Gamma \Box \Delta$ (defined analogously).

A digraph Γ is *prime* with respect to the cartesian product if the existence of an isomorphism from Γ to $\Gamma_1 \Box \Gamma_2$ implies that either Γ_1 or Γ_2 has order 1, so that Γ is isomorphic to either Γ_1 or Γ_2.

It is well known that, with respect to the cartesian product, graphs can be factorised uniquely as a product of prime factors. Digraphs also have this property. In fact, the following stronger result holds.

Theorem 2.1 (Walker, [14])**.** *Let $\Gamma_1, \ldots, \Gamma_k$, $\Gamma'_1, \ldots, \Gamma'_\ell$ be prime digraphs. If α is an isomorphism from $\Gamma_1 \Box \cdots \Box \Gamma_k$ to $\Gamma'_1 \Box \cdots \Box \Gamma'_k$, then $k = \ell$ and there exist a permutation π of $\{1, \ldots, k\}$ and isomorphisms α_i from Γ_i to $\Gamma'_{\pi(i)}$ such that α is the product of the α_is $(1 \leqslant i \leqslant k)$.*

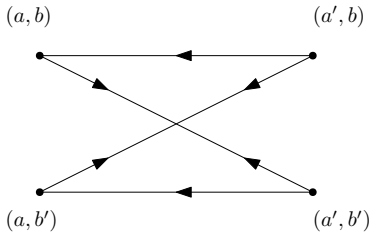
Theorem 2.1 is a corollary of [14, Theorem 10], as noted in the "Applications" section of [14]. We now present the version of Imrich's result that applies to proper digraphs.

Theorem 2.2. *If Γ is a proper digraph, then at least one of Γ or $\overline{\Gamma}$ is prime with respect to cartesian product.*

Proof. Towards a contradiction, assume that $\Gamma = \overline{A \Box B}$ and that φ is an isomorphism from Γ to $C \Box D$, where A, B, C, and D all have at least 2 vertices. A key observation is the fact that if x and y are distinct vertices in the same copy of X in a cartesian product $X \Box Y$, then every vertex contained in at least one arc with each of x and y must also lie in that copy of X.

Since Γ is a proper digraph, without loss of generality so is A, and A has an arc (a, a') such that (a', a) is not an arc of A. Let b be a vertex of B.

Pick b' to be a vertex of B distinct from b. We claim that $\varphi((a, b))$, $\varphi((a', b))$, $\varphi((a, b'))$, $\varphi((a', b'))$ all lie in some copy of either C or D. The digraph below is the subdigraph of Γ under consideration.



Since every arc in $C \Box D$ lies in either a copy of C or D, we may assume that the arc from $\varphi((a, b))$ to $\varphi((a', b'))$ lies in some copy C^d of C, say $\varphi((a, b)) = (c, d)$ and $\varphi((a', b')) = (c', d)$, with $c, c' \in \mathrm{V}(C)$ and $d \in \mathrm{V}(D)$. Towards a contradiction, suppose that $\varphi((a', b)) \notin C^d$. Then the arc from $\varphi((a', b))$ to (c, d) must lie in D^c, so $\varphi((a', b)) = (c, d')$ for some vertex d' of D. Since there is a path of length 2 via $\varphi((a, b'))$ from (c', d) to (c, d') and since $\varphi((a, b')) \neq (c, d) = \varphi((a, b))$, we must have $\varphi((a, b')) = (c', d')$. But now we have an arc from (c, d') to (c, d) and an arc from (c', d) to (c', d'), so arcs in both directions between d and d' in D. This implies that there are arcs in both directions between $(c, d) = \varphi((a, b))$

and $(c, d') = \varphi((a', b))$, a contradiction. Hence $\varphi((a', b)) \in C^d$, and by the observation in the first paragraph, we have $\varphi((a, b')) \in C^d$ also. This proves the claim.

By repeatedly applying the claim, all elements of $\varphi(\{a, a'\} \times \mathrm{V}(B))$ lie in some copy of C or D, say, C^d. Let $a'' \in \mathrm{V}(A) - \{a, a'\}$ and let b and b' be distinct vertices of B. By the definitions of cartesian product and complement, there are arcs in both directions between (a'', b) and (a, b') and between (a'', b) and (a', b'). Thus, by the observation in the first paragraph, $\varphi((a'', b))$ also lies in C^d. This shows that every vertex of Γ lies in C^d, so D is trivial. This is the desired contradiction. □

Remark 2.3. *Imrich's Theorem* [6, Theorem 1] *states that, for every graph* Γ*, either* Γ *or* $\overline{\Gamma}$ *is prime with respect to the cartesian product, with the following exceptions :* $\mathrm{K}_2\Box\mathrm{K}_2$*,* $\mathrm{K}_2\Box\overline{\mathrm{K}_2}$*,* $\mathrm{K}_2\Box\mathrm{K}_2\Box\mathrm{K}_2$*,* $\mathrm{K}_4\Box\mathrm{K}_2$*,* $\mathrm{K}_2\Box\mathrm{K}_4^-$*, and* $\mathrm{K}_3\Box\mathrm{K}_3$*, where* K_n *denotes the complete graph on* n *vertices and* K_4^- *denotes* K_4 *with an edge deleted. These would therefore be the complete list of exceptions to Theorem 2.2 if we removed the word 'proper' from the hypothesis.*

Remark 2.4. *While most of our results apply only to finite digraphs, Theorem 2.2 also applies to infinite ones (as does Imrich's Theorem). The proof is the same.*

Corollary 2.5. *Let* Γ_1 *be a proper Cayley digraph on* G *with Cayley index* i_1 *and let* Γ_2 *be a Cayley graph on* H *with Cayley index* i_2*. If* $i_1 > i_2$*, then at least one of* $\Gamma_1\Box\Gamma_2$ *or* $\overline{\Gamma_1}\Box\Gamma_2$ *has automorphism group equal to* $\mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2)$ *and, in particular, is a proper Cayley digraph on* $G \times H$ *with Cayley index* $i_1 i_2$*.*

Proof. By Theorem 2.2, one of Γ_1 and $\overline{\Gamma_1}$ is prime with respect to the cartesian product, say Γ_1 without loss of generality. Clearly, we have $\mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2) \leqslant \mathrm{Aut}(\Gamma_1\Box\Gamma_2)$. Since $i_1 > i_2$, Γ_1 cannot be a cartesian factor of Γ_2. It follows by Theorem 2.1 that every automorphism of $\Gamma_1\Box\Gamma_2$ is a product of an automorphism of Γ_1 and an automorphism of Γ_2, so that $\mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2) = \mathrm{Aut}(\Gamma_1\Box\Gamma_2)$. □

3. Additional background

The following lemma is well known and easy to prove.

Lemma 3.1. *Let* G *be a group, let* $S \subseteq G$ *and let* $\alpha \in \mathrm{Aut}(G)$*. If* $S^\alpha = S$*, then* α *induces an automorphism of* $\mathrm{Cay}(G, S)$ *which fixes the vertex corresponding to the identity.*

The next lemma is not used in any of our proofs, but it shows that the Cayley indices in Theorem 1.1 and Proposition 1.2 are as small as possible.

Lemma 3.2. *If* $\mathrm{Cay}(G, S)$ *has Cayley index* i *and* $\mathrm{Aut}(\mathrm{Cay}(G, S))$ *has at least two regular subgroups, then* G *has a proper subgroup of index at most* i*.*

Proof. Let $A = \mathrm{Aut}(\mathrm{Cay}(G, S))$ and let H be a regular subgroup of A different from G. Clearly, $G \cap H$ is a proper subgroup of G and we have $|A| \geqslant |GH| = \frac{|G||H|}{|G \cap H|}$ hence $i = |A : G| = |A : H| \geqslant |G : G \cap H|$. □

Generally, there are two notions of connectedness for digraphs: a digraph is *weakly connected* if its underlying graph is connected, and *strongly connected* if for every ordered

pair of vertices there is a directed path from the first to the second. In a finite Cayley digraph, these notions coincide (see [5, Lemma 2.6.1] for example). For this reason, we refer to Cayley digraphs as simply being *connected* or *disconnected*.

If v is vertex of a digraph Γ, then $\Gamma^+(v)$ denotes the *outneighbourhood* of v, that is, the set of vertices w of Γ such that (v, w) is an arc of Γ.

Let A be a group of automorphisms of a digraph Γ. For $v \in \mathrm{V}(\Gamma)$ and $i \geqslant 1$, we use $A_v^{+[i]}$ to denote the subgroup of A_v that fixes every vertex u for which there is a directed path of length at most i from v to u.

Lemma 3.3. *Let Γ be a connected digraph, let v be a vertex of Γ and let A be a transitive group of automorphisms of Γ. If $A_v^{+[1]} = A_v^{+[2]}$, then $A_v^{+[1]} = 1$.*

Proof. By the transitivity of A, we have $A_u^{+[1]} = A_u^{+[2]}$ for every vertex u. Using induction on i, it easily follows that, for every $i \geqslant 1$, we have $A_v^{+[i]} = A_v^{+[i+1]}$. By connectedness, this implies that $A_v^{+[1]} = 1$. □

Lemma 3.4. *Let p be a prime and let A be a permutation group whose order is a power of p. If A has a regular abelian subgroup G of index p and G has a subgroup M of index p that is normalised but not centralised by a point-stabiliser in A, then A has a regular nonabelian subgroup.*

Proof. Let A_v be a point-stabiliser in A. Note that $A = G \rtimes A_v$ and that $|A_v| = p$. Since M is normal in G and normalised by A_v, it is normal in A and has index p^2. Clearly, $M \rtimes A_v \neq G$ hence A/M contains at least two subgroups of order p and must therefore be elementary abelian.

Let α be a generator of A_v and let $g \in G - M$. By the previous paragraph, we have $(g\alpha)^p \in M$. Let $H = \langle M, g\alpha \rangle$. Since M is centralised by g but not by α, it is not centralised by $g\alpha$ hence H is nonabelian. Further, we have $|H| = p|M| = |G|$, so that H is normal in A. If H was non-regular, it would contain all point-stabilisers of A, and thus would contain α and hence also g. This would give $G = \langle M, g \rangle \leqslant H$, a contradiction. Thus H is a regular nonabelian subgroup of A. □

4. Proof of Theorem 1.1

Throughout this section, p denotes an odd prime. In Section 4.1, we show that Theorem 1.1 holds when $G \cong \mathbb{Z}_p^3$. In Sections 4.2 and 4.3, we subdivide abelian groups of rank 2 and order at least p^3 into two families, and show that the theorem holds for all such groups. Finally, in Section 4.4, we explain how these results can be applied to show that the theorem holds for all abelian groups of order at least p^3.

4.1. $\boldsymbol{G \cong \mathbb{Z}_p^3}$**.** Write $G = \langle x, y, z \rangle$, let α be the automorphism of G that maps (x, y, z) to (xy, yz, z), let $S = \{x^{\alpha^i}, y^{\alpha^i} : i \in \mathbb{Z}\}$, let $\Gamma = \mathrm{Cay}(G, S)$, and let $A = \mathrm{Aut}(\Gamma)$. Note that Γ is a proper digraph (this will be needed in Section 4.4).

It is easy to see that, for $i \in \mathbb{N}$, we have $x^{\alpha^i} = xy^i z^{\binom{i}{2}}$, $y^{\alpha^i} = yz^i$ and $z^{\alpha^i} = z$. In particular, α has order p and $|S| = 2p$. By Lemma 3.1, $G \rtimes \langle\alpha\rangle \leqslant A$. We will show that equality holds.

Using the formulas above, it is not hard to see that the induced digraph on S has exactly $2p$ arcs: $(x^{\alpha^i}, x^{\alpha^{i+1}})$ and $(y^{\alpha^i}, x^{\alpha^{i+1}})$, where $i \in \mathbb{Z}_p$. Thus, for every $s \in S$, $A_{1,s} = A_1^{+[1]}$. By vertex-transitivity, $A_{u,v} = A_u^{+[1]}$ for every arc (u, v).

Let $s \in S$. We have already seen that $A_{1,s} = A_1^{+[1]}$. Let $t \in S$. From the structure of the induced digraph on $S = \Gamma^+(1)$, we see that t has an out-neighbour in S, so that both t and this out-neighbour are fixed by $A_{1,s}$. It follows that $A_{1,s}$ fixes all out-neighbours of t. We have shown that $A_{1,s} = A_1^{+[2]}$. By Lemma 3.3, it follows that $A_{1,s} = 1$. Since the induced digraph on S is not vertex-transitive and $\alpha \in A_1$, the A_1-orbits on S have length p. Hence $|A_1| = p|A_{1,s}| = p$. Thus, Γ has Cayley index p and $A = G \rtimes \langle\alpha\rangle$. Finally, we apply Lemma 3.4 with $M = \langle y, z\rangle$ to deduce that A contains a nonabelian regular subgroup.

4.2. $\boldsymbol{G \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_p}$ **with** $\boldsymbol{n \geqslant 2}$**.** Write $G = \langle x, y\rangle$, let $x_0 = x^{p^{n-1}}$, let α be the automorphism of G that maps (x, y) to (xy, x_0y), let $S = \{x^{\alpha^i}, y^{\alpha^i} : i \in \mathbb{Z}\}$ and let $\Gamma = \mathrm{Cay}(G, S)$. Again, note that Γ is a proper digraph.

Since $n \geqslant 2$, x_0 is fixed by α. It follows that, for $i \in \mathbb{N}$, we have $x^{\alpha^i} = xy^i x_0^{\binom{i}{2}}$ and $y^{\alpha^i} = yx_0^i$. In particular, α has order p and $|S| = 2p$.

Using these formulas, it is not hard to see that the induced digraph on S has exactly $2p$ arcs: $(x^{\alpha^i}, x^{\alpha^{i+1}})$ and $(y^{\alpha^i}, x^{\alpha^{i+1}})$, where $i \in \mathbb{Z}_p$. The proof is now exactly as in the previous section, except that we use $M = \langle x^p, y\rangle$ when applying Lemma 3.4.

4.3. $\boldsymbol{G \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}}$ **with** $\boldsymbol{n \geqslant m \geqslant 2}$**.** Write $G = \langle x, y\rangle$, let $x_0 = x^{p^{n-1}}$, let $y_0 = y^{p^{m-1}}$, let α be the automorphism of G that maps (x, y) to (xy_0, yx_0), let $S = \{x^{\alpha^i}, y^{\alpha^i}, (xy^{-1})^{\alpha^i} : i \in \mathbb{Z}\}$, let $\Gamma = \mathrm{Cay}(G, S)$, and let $A = \mathrm{Aut}(\Gamma)$. Again, note that Γ is a proper digraph.

Since $n \geqslant m \geqslant 2$, x_0 and y_0 are both fixed by α. It follows that, for $i \in \mathbb{N}$, we have $x^{\alpha^i} = xy_0^i$, and $y^{\alpha^i} = yx_0^i$. In particular, α has order p and $|S| = 3p$. By Lemma 3.1, $G \rtimes \langle\alpha\rangle \leqslant A$.

Using the formulas above, it is not hard to see that the induced digraph on S has exactly $2p$ arcs: $((xy^{-1})^{\alpha^i}, x^{\alpha^i})$ and $(y^{\alpha^i}, x^{\alpha^i})$, where $i \in \mathbb{Z}_p$. It follows that $|A_1 : A_{1,x}| = p$. We will show that $A_{1,x} = 1$, which will imply that $A = G \rtimes \langle\alpha\rangle$.

Let $X = \{x^{\alpha^i} : i \in \mathbb{Z}\} = x\langle y_0\rangle$, $Y = \{x^{\alpha^i} : i \in \mathbb{Z}\} = y\langle x_0\rangle$ and $Z = \{(xy^{-1})^{\alpha^i} : i \in \mathbb{Z}\} = xy^{-1}\langle x_0^{-1}y_0\rangle$. It follows from the previous paragraph that X is an orbit of A_1 on S.

Note that the p elements of $Y^2 = y^2\langle x_0\rangle$ are out-neighbours of every element of Y. Similarly, the p elements of Z^2 are out-neighbours of every element of Z. On the other hand, one can check that an element of Y and an element of Z have a unique out-neighbour in common, namely their product. This shows that Y and Z are blocks for A_1. We claim that Y and Z are orbits of A_1.

Let $Y_1 = Y$ and, for $i \geqslant 2$, inductively define $Y_i = \bigcap_{x \in Y_{i-1}} \Gamma^+(x)$. Define Z_i analogously. Let $g \in A_1$. By induction, $Y_i^g \in \{Y_i, Z_i\}$, and $Y_i^g = Z_i$ if and only if $Y^g = Z$. Note that $Y_i = Y^i = y^i\langle x_0\rangle$ and $Z_i = Z^i = x^i y^{-i}\langle x_0^{-1}y_0\rangle$. If $n = m$, then $1 \in x_0 y_0^{-1}\langle x_0^{-1}y_0\rangle = Z_{p^{m-1}}$, but $1 \notin y_0\langle x_0\rangle = Y_{p^{m-1}}$, so Y and Z are orbits for A_1. We may thus assume that $n > m$. Note that $y_0 \in y_0\langle x_0\rangle = Y_{p^{m-1}}$, and y_0 is an in-neighbour of $x \in X$. However, $Z_{p^{m-1}} = x^{p^{m-1}} y_0^{-1}\langle x_0^{-1}y_0\rangle$. Since $n > m$, we see that no vertex of $Z_{p^{m-1}}$ is an in-neighbour of a vertex of X. Again it follows that Y and Z are orbits for A_1.

Considering the structure of the induced digraph on S, it follows that, for every $s \in S$, $A_{1,s} = A_1^{+[1]}$. By vertex-transitivity, $A_{u,v} = A_u^{+[1]}$ for every arc (u, v). Since elements of Y and Z have an out-neighbour in S, $A_{1,x}$ fixes the out-neighbours of elements of Y and Z. Furthermore, for every $i \in \mathbb{Z}$, $xy_0^i y$ is a common outneighbour of xy_0^i and y, hence it is fixed by $A_{1,x}$. Thus, every element of X has an out-neighbour fixed by $A_{1,x}$. It follows that $A_{1,x}$ fixes all out-neighbours of elements of X and thus $A_{1,x} = A_1^{+[1]} = A_1^{+[2]}$. By Lemma 3.3, it follows that $A_{1,x} = 1$. As in Section 4.1, we can also conclude $|A_1| = p$, Γ has Cayley index p and $A = G \rtimes \langle\alpha\rangle$. Finally, applying Lemma 3.4 with $M = \langle x^p, y\rangle$ implies that A contains a nonabelian regular subgroup.

4.4. **General case.** Recall that G is an abelian p-group that has order at least p^3 and is not cyclic. By the Fundamental Theorem of Finite Abelian Groups, we can write $G = G_1 \times G_2$, where G_1 falls into one of the three cases that have already been dealt with in this section.

(More explicitly, if G is not elementary abelian, then we can take G_1 isomorphic to $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ with $n \geqslant 2$ and $m \geqslant 1$. If G is elementary abelian, then, since $|G| \geqslant p^3$, we can take G_1 isomorphic to $\mathbb{Z}_p^3$.)

We showed in the previous three sections that there exists a proper Cayley digraph Γ_1 on G_1 with Cayley index equal to p and whose automorphism group contains a nonabelian regular subgroup.

Note that every cyclic group admits a Cayley digraph whose Cayley index is 1. (For example, the directed cycle of the corresponding order.) Since G_2 is a direct product of cyclic groups, applying Corollary 2.5 iteratively yields a proper Cayley digraph Γ on $G_1 \times G_2$ with automorphism group $\mathrm{Aut}(\Gamma_1) \times G_2$. In particular, Γ has Cayley index p and its automorphism group contains a nonabelian regular subgroup. This concludes the proof of Theorem 1.1.

In fact, the proof above yields the following stronger result.

Theorem 4.1. *Let G be an abelian group. If there is an odd prime p such that the Sylow p-subgroup of G is neither cyclic nor elementary abelian of rank 2, then G admits a proper Cayley digraph with Cayley index p whose automorphism group contains a nonabelian regular subgroup.*

5. Proof of Proposition 1.2

We begin with a lemma that helps to establish the existence of regular subgroups.

Lemma 5.1. *Let G be a group with nontrivial subgroups H and B such that $G = HB$ and $H \cap B = 1$, and let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph on G. If S is closed under conjugation by B, then $\mathrm{Aut}(\Gamma)$ has a regular subgroup distinct from the right regular representation of G and isomorphic to $H \times B$.*

Proof. Let $A = \mathrm{Aut}(\Gamma)$. For $g \in G$, let ℓ_g and r_g denote the permutations of G induced by left and right multiplication by g, respectively. Similarly, for $g \in G$, let c_g denote the permutation of G induced by conjugation by g. For $X \leqslant G$, let $R_X = \langle r_x : x \in X \rangle$. Let $L_B = \langle \ell_b : b \in B \rangle$ and $C_B = \langle c_b : b \in B \rangle$. Note that $R_H \leqslant A$. For every $g \in G$, $r_g c_{g^{-1}} = \ell_g$. For all $b \in B$, we have $r_b \in A$ and, since S is closed under conjugation by B, $c_{b^{-1}} \in A$ hence $L_B \leqslant A$.

Let $K = \langle L_B, R_H \rangle$. If $K = R_G$, then $L_B \leqslant R_G$ which implies that $C_B \leqslant R_G$, contradicting the fact that R_G is regular. Thus $K \neq R_G$. Note that L_B and R_H commute. Suppose that $k \in R_H \cap L_B$, so $k = r_h = \ell_b$ for some $h \in H$ and some $b \in B$. Thus

$$h = 1^{r_h} = 1^k = 1^{\ell_b} = b.$$

Since $H \cap B = 1$, this implies $k = 1$. It follows that $R_H \cap L_B = 1$ and hence $K = R_H \times L_B \cong H \times B$. Finally, suppose that some $k = r_h \ell_b \in K$ fixes 1. It follows that $1^{r_h \ell_b} = 1 = bh$ so that $b \in H$, a contradiction. This implies that K is regular, which concludes the proof. □

We now prove a general result, which together with Lemma 5.1 will imply Proposition 1.2.

Proposition 5.2. *Let G be a group generated by an involution x and an element y of order 3, let $S = \{x, y, y^x\}$ and let $\Gamma = \mathrm{Cay}(G, S)$. If G is isomorphic to neither $\mathbb{Z}_6$ nor $\mathbb{Z}_3 \wr \mathbb{Z}_2 \cong \mathbb{Z}_3^2 \rtimes \mathbb{Z}_2$, then Γ has Cayley index 2.*

Proof. Clearly, Γ is connected. Since G is not isomorphic to $\mathbb{Z}_6$, we have $y^x \neq y$. In particular, we have $|S| = 3$. If $y^x = y^{-1}$, then $G \cong \mathrm{Sym}(3)$ and the result can be checked directly. We therefore assume that $y^x \neq y^{-1}$. Since $G \ncong \mathbb{Z}_3 \wr \mathbb{Z}_2$, we have $y^x y \neq y y^x$.

We have that $\Gamma^+(x) = \{1, yx, xy\}$, $\Gamma^+(y) = \{xy, y^2, y^x y\}$ and $\Gamma^+(y^x) = \{yx, yy^x, (y^2)^x\}$. One can check that the only equalities between elements of these sets are the ones between elements having the same representation. In other words, $|\{1, yx, xy, y^2, y^x y, yy^x, (y^2)^x\}| = 7$. (For example, if $yx = y^x y$, then $x^{y^{-1}} = y^x$, contradicting the fact that x and y have different orders.)

Let $A = \mathrm{Aut}(\Gamma)$ and let c_x denote conjugation by x. Note that $c_x \in A_1$. We first show that $A_1^{+[1]} = 1$. It can be checked that y^2 is the unique out-neighbour of y that is also an in-neighbour of 1, hence it is fixed by $A_1^{+[1]}$, and so is $(y^2)^x$ by analogous reasoning. We have seen earlier that xy is the unique common out-neighbour of x and y, hence it too is fixed by $A_1^{+[1]}$, and similarly for yx. Being the only remaining out-neighbours of y, $y^x y$ must be also fixed, and similarly for yy^x. Thus $A_1^{+[1]} = A_1^{+[2]}$. Since Γ is connected, Lemma 3.3 implies that $A_1^{+[1]} = 1$.

Note that x is the only out-neighbour of 1 that is also an in-neighbour, hence it is fixed by A_1, whereas c_x interchanges y and y^x. It follows that $|A_1| = |A_1 : A_1^{+[1]}| = 2$ and Γ has Cayley index 2, as desired. □

Proof of Proposition 1.2. Let $\Gamma = \mathrm{Cay}(G, \{x, y, y^x\})$. By Proposition 5.2, Γ has Cayley index 2. Since $|G : H| = 2$ and y has order 3, we have $y \in H$. As $\langle x, y\rangle = G$, we have $x \notin H$ and $G = H \rtimes \langle x\rangle$. Clearly, $\{x, y, y^x\}$ is closed under conjugation by x. It follows by Lemma 5.1 that $\mathrm{Aut}(\Gamma)$ has a regular subgroup distinct from G and isomorphic to $H \times \langle x\rangle \cong H \times \mathbb{Z}_2$. □

It was shown by Miller [10] that, when $n \geqslant 9$, $\mathrm{Sym}(n)$ admits a generating set consisting of an element of order 2 and one of order 3; this is also true when $n \in \{3, 4\}$. In these cases, we can apply Proposition 1.2 with $H = \mathrm{Alt}(n)$ to obtain a Cayley digraph on $\mathrm{Sym}(n)$ that has Cayley index 2 and whose automorphism group contains a regular subgroup isomorphic to $\mathrm{Alt}(n) \times \mathbb{Z}_2$.

A short alternate proof of this fact can be derived from a result of Feng [4]. This yields a Cayley graph and is valid for $n \geqslant 5$.

Proposition 5.3. *If $n \geqslant 5$, then there is a Cayley graph on $\mathrm{Sym}(n)$ with Cayley index 2, whose automorphism group contains a regular subgroup isomorphic to $\mathrm{Alt}(n) \times \mathbb{Z}_2$.*

Proof. Let $T = \{(1\ 2), (2\ 3), (2\ 4)\} \cup \{(i\ i{+}1) : 4 \leqslant i \leqslant n{-}1\}$ and let $\Gamma = \mathrm{Cay}(\mathrm{Sym}(n), T)$. Note that all elements of T are transpositions. Let $\mathrm{Tra}(T)$ be the transposition graph of T, that is, the graph with vertex-set $\{1, \ldots, n\}$ and with an edge $\{i, j\}$ if and only if $(i\ j) \in T$. Note that $\mathrm{Tra}(T)$ is a tree and thus T is a minimal generating set for $\mathrm{Sym}(n)$ (see for example [5, Section 3.10]). Let $B = \langle(1\ 3)\rangle$. Since $n \geqslant 5$, $\mathrm{Aut}(\mathrm{Tra}(T)) = B$. It follows by [4, Theorem 2.1] that $\mathrm{Aut}(\Gamma) \cong \mathrm{Sym}(n) \rtimes B$. In particular, Γ has Cayley index 2.

Note that $\mathrm{Sym}(n) = \mathrm{Alt}(n) \rtimes B$ and that T is closed under conjugation by B. Applying Lemma 5.1 with $H = \mathrm{Alt}(n)$ shows that $\mathrm{Aut}(\Gamma)$ has a regular subgroup isomorphic to $\mathrm{Alt}(n) \times \mathbb{Z}_2$. □

References

[1] Brian Alspach and Shaofei Du. Suborbit structure of permutation p-groups and an application to Cayley digraph isomorphism. *Canad. Math. Bull.* **47** (2004), 161–167.

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

[3] John Bamberg and Michael Giudici. Point regular groups of automorphisms of generalised quadrangles. *J. Combin. Theory Ser. A* **118** (2011), 1114–1128.

[4] Yan-Quan Feng. Automorphism groups of Cayley graphs on symmetric groups with generating transposition sets. *J. Combin. Theory Ser. B* **96** (2006), 67–72.

[5] Chris Godsil and Gordon Royle. Algebraic graph theory. Graduate Texts in Mathematics, 207. Springer-Verlag, New York, 2001.

[6] Wilfried Imrich. On products of graphs and regular groups. *Israel J. Math* **11** (1972), 258–264.

[7] Anne Joseph. The isomorphism problem for Cayley digraphs on groups of prime-squared order. *Discrete Math.* **141** (1995), 173–183.

[8] István Kovács and Mary Servatius. On Cayley digraphs on nonisomorphic 2-groups. *J. Graph Theory* **70** (2012), 435–448.
[9] Dragan Marušič and Joy Morris. Normal circulant graphs with noncyclic regular subgroups. *J. Graph Theory* **50** (2005), 13–24.
[10] G. A. Miller. On the groups generated by two operators. *Bull. Amer. Math. Soc.* **7** (1901), 424–426.
[11] Joy Morris. Isomorphic Cayley graphs on nonisomorphic groups. *J. Graph Theory* **31** (1999), 345–362.
[12] Gordon Royle. A Normal Non-Cayley-Invariant Graph for the Elementary Abelian Group of Order 64. *J. Aust. Math. Soc.* **85** (2008), 347–351.
[13] Pablo Spiga. Enumerating groups acting regularly on a d-dimensional cube. *Comm. Algebra* **37** (2009), 2540–2545.
[14] James W. Walker. Strict refinement for graphs and digraphs. *J. Combin. Theory Ser. B* **43** (1987), 140–150.
[15] Boris Zgrablić. On quasiabelian Cayley graphs and graphical doubly regular representations. *Discrete Math.* **244** (2002), 495–519.

Luke Morgan, School of Mathematics and Statistics (M019), University of Western Australia, Crawley, 6009, Australia
E-mail address: luke.morgan@uwa.edu.au

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

Gabriel Verret, Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland 1142, New Zealand.
E-mail address: g.verret@auckland.ac.nz