Isomorphic Cayley Graphs on Nonisomorphic Groups

Joy Morris
Department of Mathematics and Statistics,
Simon Fraser University,
Burnaby, BC. V5A 1S6. CANADA.
morris@cs.sfu.ca

January 12, 2004

Abstract:
The issue of when two Cayley digraphs on different abelian groups of prime power order can be isomorphic is examined. This had previously been determined by Anne Joseph for squares of primes; her results are extended.

1 Preliminaries

We begin with some essential definitions. For many of the results in this paper, the lemmata and proofs used are direct extensions of those in Joseph's paper [1]. For background and definitions not provided within the paper, see [2] or [5]. Although we are dealing with abelian groups, multiplicative notation will be used.

Let S be a subset of a group G. The *Cayley digraph* $X = X(G;S)$ is the directed graph given as follows. The vertices of X are the elements of the group G. There is an arc between two vertices g and h if and only if $g^{-1}h \in S$. In other words, for every vertex $g \in G$ and element $s \in S$, there is an arc from g to gs.

Notice that if the identity element 1 of G is in S, then there is a loop at every vertex, while if $1 \notin S$, the digraph has no loops. For convenience, we will assume the latter case holds; it makes no difference to the results. Also notice that since S is a set, it contains no multiple entries and hence there are no multiple arcs.

A Cayley digraph can be considered to be a *Cayley graph* if whenever

$s \in S$, we also have $s^{-1} \in S$, since in this case every arc is part of a digon, and we can replace the digons with undirected edges.

The *wreath product* of two digraphs X and Y, written $X \wr Y$, is given as follows. The vertices of the new digraph are all pairs (x, y) where x is a vertex of X and y is a vertex of Y. The arcs of $X \wr Y$ are given by the pairs $\{[(x_1, y_1), (x_1, y_2)] : [y_1, y_2]$ is an arc of $Y\}$ together with $\{[(x_1, y_1), (x_2, y_2)] : [x_1, x_2]$ is an arc of $X\}$. In other words, there is a copy of the digraph Y for every vertex of X, and arcs exist from one copy of Y to another if and only if there is an arc in the same direction between the corresponding vertices of X. If any arcs exist from one copy of Y to another, then all arcs exist in that direction between those copies of Y.

We define a partial order on the set of abelian groups of order p^n, as follows. We say $G \leq_{po} H$ if there is a chain

$$H_1 < H_2 < \ldots < H_m = H$$

of subgroups of H, such that H_1, $\frac{H_2}{H_1}$, $\ldots$, $\frac{H_m}{H_{m-1}}$ are all cyclic, and

$$G \cong H_1 \times \frac{H_2}{H_1} \times \ldots \times \frac{H_m}{H_{m-1}}.$$

There is an equivalent definition for this partial order that is less group-theoretic but perhaps more intuitive. We say that a string of integers $i_1, \ldots, i_m$ is a *subdivision* of the string of integers $j_1, \ldots, j_{m'}$ if there is some permutation δ of $\{1, \ldots, m\}$ and some strictly increasing sequence of integers $0 = k_0, \ldots, k_t = m$ such that $i_{\delta(k_s+1)} + \ldots + i_{\delta(k_{s+1})} = j_{s+1}$, $0 \leq s \leq m' - 1$. Now, $G \leq_{po} H$ precisely if $G \cong \mathbf{Z}_{p^{i_1}} \times \mathbf{Z}_{p^{i_2}} \times \ldots \times \mathbf{Z}_{p^{i_m}}$ and $H \cong \mathbf{Z}_{p^{j_1}} \times \mathbf{Z}_{p^{j_2}} \times \ldots \times \mathbf{Z}_{p^{j_{m'}}}$ where $i_1, \ldots, i_m$ is a subdivision of $j_1, \ldots, j_{m'}$.

Figure 1 illustrates this partial order on abelian groups of order p^5.

We are now ready to give the main result, which will be proven in the succeeding sections.

Theorem 1.1 *Let $X = X(G; S)$ be a Cayley digraph on an abelian group G of order p^n, where p is an odd prime. Then the following are equivalent:*

1. *The digraph X is isomorphic to a Cayley digraph on both $\mathbf{Z}_{p^n}$ and H, where H is an abelian group with $|H| = p^n$, say*

   $$H = \mathbf{Z}_{p^{k_1}} \times \mathbf{Z}_{p^{k_2}} \times \ldots \times \mathbf{Z}_{p^{k_{m'}}}$$

   where $k_1 + \ldots + k_{m'} = n$.

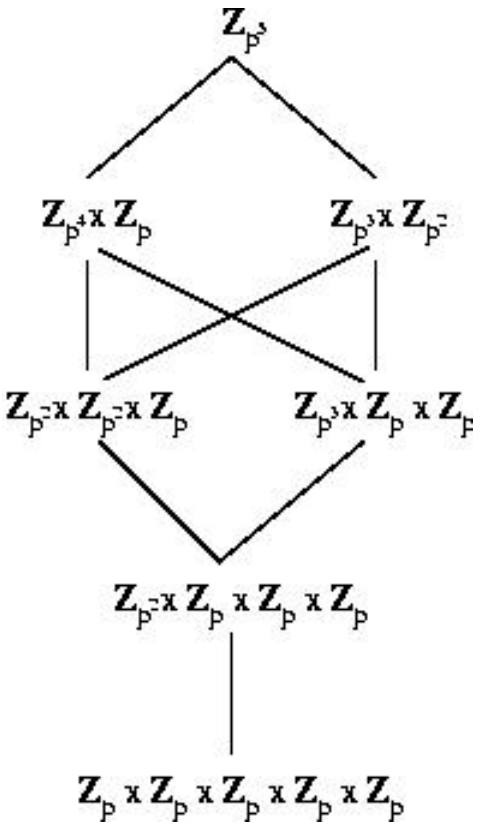

Figure 1: The partial order for abelian groups of order p^5.

2. *There exist a chain of subgroups* $G_1 \subset \ldots \subset G_{m-1}$ *in* G *such that*

   (a) $G_1, \frac{G_2}{G_1}, \ldots, \frac{G}{G_{m-1}}$ *are cyclic groups;*

   (b) $G_1 \times \frac{G_2}{G_1} \times \ldots \times \frac{G}{G_{m-1}} \leq_{po} H$;

   (c) *For all* $s \in S \setminus G_i$, *we have* $sG_i \subseteq S$, *for* $i = 1, \ldots, m-1$. *(That is,* $S \setminus G_i$ *is a union of cosets of* G_i*.)*

3. *There exist Cayley digraphs* $U_1, \ldots, U_m$ *on cyclic* p*-groups* $H_1, \ldots, H_m$ *such that* $H_1 \times \ldots \times H_m \leq_{po} H$ *and* $X \cong U_m \wr \ldots \wr U_1$.

These in turn imply:

4. X *is isomorphic to Cayley digraphs on every abelian group of order* p^n *that is greater than* H *in the partial order.*

This theorem provides several conditions for determining whether or not a given Cayley digraph on an abelian group can be represented as a Cayley digraph on other abelian groups of the same odd prime power order.

Let us look at some simple examples of the use of this theorem. Let

$$G = \mathbf{Z}_9 \times \mathbf{Z}_3 \times \mathbf{Z}_3.$$

Let

$$S = \{(2, i, j), (5, i, j), (8, i, j), (0, i, 2), (0, 1, 0) : 0 \leq i, j \leq 2\}.$$

Then G and S satisfy condition (2) with $G_1 = \langle (0, 1, 0) \rangle$, $G_2 = \langle G_1, (0, 0, 1) \rangle$, $G_3 = \langle G_2, (3, 0, 0) \rangle$, and $H = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$. So (due to condition (4)) $X(G; S)$ can be represented as a Cayley digraph on any abelian group of order 81.

Alternatively, consider the same group G with

$$S = \{(2, i, j), (5, i, j), (8, i, j), (0, 1, 1), (0, 1, 2) : 0 \leq i, j \leq 2\}.$$

There is no cyclic subgroup G_1 of G that will satisfy condition (2c), so the digraph $X(G; S)$ cannot be represented as a Cayley digraph on the cyclic group of order 81.

Condition (3) is more of a visual condition, stating that the digraph X is a Cayley digraph on both the cyclic group and some other abelian group of order p^n, if and only if it can be drawn as the wreath product of a sequence of Cayley digraphs on smaller cyclic groups.

The next two sections, which prove $3 \Rightarrow 1, 4$ and $2 \Rightarrow 3$, are based very closely on Joseph's paper. In Section 4, which proves that $1 \Rightarrow 2$, the

proof follows the same outline as Joseph's (although some of the methods required are slightly different), through Lemma 4.4. From that point on, the lemmata and proofs diverge significantly from those in her paper. These three sections complete the proof of Theorem 1.1. Section 5 deals with the case where $p = 2$, and section 6 gives a slightly weaker result following from the same proof, for the case where G is not abelian. Section 7 considers the possibility of further extensions of these results.

2 Proof of $3 \Rightarrow 1, 4$

Throughout the proof of the main result, we will generally be using induction. The base case is $n = 1$, and is trivially true. Again, we begin this section with some necessary preliminaries.

Theorem 2.1 (See [3], Lemma 4.) *Let X be a digraph and G be a group. The automorphism group $Aut(X)$ has a subgroup isomorphic to G that acts regularly on $V(X)$ if and only if X is isomorphic to a Cayley digraph $X(G; S)$ for some subset S of G.*

Although the proof in Sabidussi's paper is given for graphs rather than digraphs, it works for both structures.

We also require the notion of wreath product of permutation groups. (See [4], pg. 693.) Let U and V be sets, H and K groups of permutations of U and V respectively. The *wreath product* $H \wr K$ is the group of all permutations f of $U \times V$ for which there exist $h \in H$ and an element k_u of K for each $u \in U$ such that

$$f((u, v)) = (h(u), k_{h(u)}(v))$$

for all $(u, v) \in U \times V$.

Lemma 2.2 (See [4], pg. 694.) *Let U and V be digraphs. Then the group $Aut(U) \wr Aut(V)$ is contained in the group $Aut(U \wr V)$.*

(This follows immediately from the definition of wreath product of permutation groups, and is mentioned only as an aside in Sabidussi's paper and in the context of graphs. It is equally straightforward for digraphs.)

Once we have noted that the wreath product of permutation groups is associative, we are ready to proceed with our proof.

Proof of $3 \Rightarrow 1, 4$. Let us define v_j $(1 \leq j \leq m)$ to be the number

of vertices in U_j (which is a power of p). We may assume that the digraph U_j has vertices labeled with $0, 1, \ldots, v_j - 1$ in such a way that the permutation σ defined by $\sigma(x) = x + 1 \pmod{v_j}$ is an automorphism of the digraph. It is sufficient, by Theorem 2.1 above, to find a regular subgroup of $\mathrm{Aut}(X)$ that is isomorphic to the group

$$\mathbf{Z}_{v_i v_j} \times H_1 \times \ldots \times H_{i-1} \times H_{i+1} \times \ldots \times H_{j-1} \times H_{j+1} \times \ldots \times H_m,$$

for each pair (i, j) satisfying $1 \leq i < j \leq m$. This is because every abelian group of order p^n that is greater than $H_1 \times H_2 \times \ldots \times H_m$ in the partial order, can be obtained by repeating the step of combining two elements in the direct product, with appropriate choices of i and j. Since H is greater than or equal to $H_1 \times H_2 \times \ldots \times H_m$, the result will be achieved if such regular subgroups of $\mathrm{Aut}(X)$ are shown to exist.

Now, by repeated use of Lemma 2.2 above, we see that

$$\mathrm{Aut}(U_1) \wr \mathrm{Aut}(U_2) \wr \ldots \wr \mathrm{Aut}(U_m) \subseteq \mathrm{Aut}(U_1 \wr U_2 \wr \ldots \wr U_m) = \mathrm{Aut}(X),$$

so if we can find the required regular subgroups in

$$\mathrm{Aut}(U_1) \wr \mathrm{Aut}(U_2) \wr \ldots \wr \mathrm{Aut}(U_m),$$

we will be done. We will do this by finding independent cycles of lengths

$$v_i v_j, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{j-1}, v_{j+1}, \ldots, v_m.$$

The cycle of length v_k will affect only the vertices of U_k $(1 \leq k \leq m, k \neq i, j)$. The cycle is defined as follows. It is not hard to see that the map

$$f_k((u_1, \ldots, u_k, \ldots, u_m)) = (u_1, \ldots, u_k + 1, \ldots, u_m)$$

(where addition is done modulo v_j) is in the group

$$\mathrm{Aut}(U_1) \wr \mathrm{Aut}(U_2) \wr \ldots \wr \mathrm{Aut}(U_m).$$

These are clearly independent cycles. Now we will replace the cycles f_i and f_j by a single cycle $g_{i,j}$ of length $v_i v_j$ which is also in $\mathrm{Aut}(X)$. Let f_i' be the restriction of f_i to $U_1 \wr \ldots \wr U_{j-1}$, and f_j'' be the restriction of f_j to $U_j \wr \ldots \wr U_m$. Define f'_{j,u_i} to be equal to f_j'' if the given value u_i is equal to $v_i - 1$, and to be the identity otherwise. Then define

$$g_{i,j}(u_1, \ldots, u_m) = (f_i'(u_1, \ldots, u_{j-1}), f'_{j,u_i}(u_j, \ldots, u_m)).$$

It is clear from the definition of wreath products of groups that this will be in $\mathrm{Aut}(X)$, and it is not hard to see that it is indeed a cycle of the required length which is independent of the other cycles we have created.

The group generated by these cycles is certainly regular on the digraph X, so the result follows. ■

3 Proof of $2 \Rightarrow 3$

Let Y be a subset of $V(X)$, where X is a digraph. We denote the induced subdigraph of X on the vertices in the set Y by $X[Y]$.

We copy a very nice lemma from the Joseph paper.

Lemma 3.1 (See [1], Lemma 3.11.) *Let X and $\overline{X}$ be digraphs. Let $\phi : V(X) \to V(\overline{X})$ be a surjective map. Assume the following conditions are satisfied:*

1. *For every v and w in $V(\overline{X})$, the induced subdigraph $X[\phi^{-1}(v)]$ is isomorphic to the induced subdigraph $X[\phi^{-1}(w)]$.*
2. *For every x and y in $V(X)$ with $\phi(x) \neq \phi(y)$, the vertex x is adjacent to the vertex y in X if and only if $\phi(x)$ is adjacent to $\phi(y)$ in $\overline{X}$.*

Then $X \cong \overline{X} \wr X[\phi^{-1}(v_0)]$ for every $v_0 \in V(\overline{X})$.

The proof of this result is a simple matter of defining an isomorphism, together with induction.

Proof of $2 \Rightarrow 3$. Define a digraph $\overline{X}$ on the cosets of G_{m-1} by

$$V(\overline{X}) = \{G_{m-1}x : x \in G\}$$

and the arcs of the digraph are

$$A(X) = \{[G_{m-1}x, G_{m-1}y] : x^{-1}y \in S \setminus G_{m-1}\}.$$

Since $S \setminus G_{m-1}$ is a union of cosets of G_{m-1}, these arcs are well-defined. It is not hard to see from this definition that $\overline{X}$ (which we will call U_m) is a Cayley digraph on $\frac{G}{G_{m-1}}$.

Now define the map $\phi : V(X) \to V(\overline{X})$ by $\phi(x) = G_{m-1}x$. The conditions in Lemma 3.1 above are satisfied, so we have $X \cong \overline{X} \wr X[G_{m-1}]$. Now the induced subdigraph $X[G_{m-1}]$ is just the Cayley digraph $X(G_{m-1}; S \bigcap G_{m-1})$. With the subgroups $G_1, \ldots, G_{m-2}$, this second Cayley digraph satisfies condition (2) of Theorem 1.1, but has $|G_{m-1}|$ vertices. By induction, we can assume that this digraph $X[G_{m-1}]$ is the wreath product of Cayley digraphs $U_{m-1}, \ldots, U_1$ on the groups $\frac{G_{m-1}}{G_{m-2}}, \ldots, G_1$ respectively.

Now

$$X \cong \overline{X} \wr X[G_{m-1}] \cong U_m \wr U_{m-1} \wr \ldots \wr U_1$$

is as required. ■

4 Proof of $1 \Rightarrow 2$

We are now assuming that condition (1) of the main result holds.

Lemma 4.1 *The Sylow p-subgroups of Aut(X) contain regular subgroups Q and R that are isomorphic to $\mathbf{Z}_{p^n}$ and H, respectively. Thus the Sylow p-subgroups have order at least p^{n+1}.*

PROOF. Since X is a Cayley digraph on both $\mathbf{Z}_{p^n}$ and H, the group $\mathrm{Aut}(X)$ contains regular subgroups that are isomorphic to $\mathbf{Z}_{p^n}$, and others isomorphic to H. These are certainly contained in Sylow p-subgroups, and since all Sylow p-subgroups are conjugate, each Sylow p-subgroup must contain at least one subgroup isomorphic to each of $\mathbf{Z}_{p^n}$ and H. We call these Q and R.

Since both of these groups are in a Sylow p-subgroup, and they are nonisomorphic, the Sylow p-subgroup must have order at least p^{n+1}.■

The Sylow p-subgroup under examination, which contains subgroups $Q \cong \mathbf{Z}_{p^n}$ and $R \cong H$, will be denoted P.

In a set X under the action of a group G, a subset B is called a *G-block* if for each $g \in G$, either $g(B) = B$ or $g(B) \bigcap B = \emptyset$. If furthermore $|B| > 1$ and B is a proper subset of X, then the G-block B is called *nontrivial*.

The group G is *imprimitive* in its action on the set X if nontrivial G-blocks exist.

Notice that when G is transitive, the elements of X can be partitioned into blocks of a single size, by taking all of the images under G of a fixed block.

Notice that the action of Q on X produces unique partitions of the elements of X into blocks of any size $p^m, 1 \leq m \leq n-1$. If the vertices of X are labeled with $0, 1, \ldots, p^n - 1$ in such a way that addition modulo p^n has the same action on X as Q has, then the blocks of size p^m are precisely the congruence classes modulo p^{n-m}.

Theorem 4.2 (See [5], pg. 13) *If the transitive group P contains an intransitive normal subgroup N different from 1, then P is imprimitive. The orbits of N are P-blocks.*

Lemma 4.3 *Every Q-block is a P-block, and vice versa.*

PROOF. Clearly since $Q \subseteq P$, every P-block is a Q-block. We will use induction, and show that if P has blocks of size p^{i-1} that are the orbits of a normal subgroup of order p^{i-1} in P, then P has blocks of size p^i that

are orbits of a normal subgroup of order p^i in P, where $i < n$. Then since there are P-blocks of every possible size, and since these P-blocks are also Q-blocks, and since the Q blocks of any given size are unique, every Q-block must be a P-block.

We will be using Theorem 4.2 heavily, so it is useful to point out that P is indeed transitive, and due to size alone, the normal subgroups we will consider must be intransitive. In the base case $i = 1$, this is straightforward: P itself is a non-trivial p-group, so has a non-trivial center by a well-known result, which is itself a p-group and so must have an element of order p. This element generates a subgroup of order p within the center of P, which is certainly normal in P. By Theorem 4.2, the orbits of this group are P-blocks.

We will denote the normal subgroup of order p^{i-1} by $P^{(i-1)}$. We look at the group $P/P^{(i-1)}$. This is a non-trivial p-group since $i < n$, so by a well-known result, it has a non-trivial center. The center is a p-group, so certainly has an element of order p, g (say). Now look at $\langle P^{(i-1)}, g\rangle$. First, this is normal in P since if

$$h \in aP^{(i-1)} \subseteq G,$$

then

$$h^{-1}gh \in P^{(i-1)}a^{-1}gaP^{(i-1)}$$

and since g is in the center of $P/P^{(i-1)}$, this means

$$h^{-1}gh \in gP^{(i-1)} \subseteq \langle P^{(i-1)}, g\rangle.$$

Also, the orbits have length p^i since the action of g combines sets of p orbits of $P^{(i-1)}$, each of which had length p^{i-1} by assumption. Hence $\langle P^{(i-1)}, g\rangle$ is an intransitive, normal, non-trivial subgroup of P, whence by Theorem 4.2, each of its orbits is a P-block.

As these are P-blocks of size p^i, they must also be Q-blocks, and hence be the unique Q-blocks of size p^i already described. Since this has shown that P has blocks of every order p^i $(1 \leq i \leq n-1)$, every Q-block is indeed a P-block. ■

We will denote the P-block of size p^i that contains the vertex x by $B_{x,i}$.

In the permutation group G acting on the set X, the *stabilizer subgroup* of the element $x \in X$ is the subgroup of G containing all group elements that fix the element x. It is generally denoted by $\mathrm{Stab}_G(x)$, or more simply, G_x.

Lemma 4.4 *If x and y are two vertices in the same P-block of size p (that is, $y \in B_{x,1}$), then $P_x = P_y$.*

PROOF. Since the group P_x fixes the vertex x, it must fix the block $B_{x,1}$ setwise. Since P_x is a p-group, all orbits must have length a power of p, so each of the other $p-1$ elements of $B_{x,1}$, including y, must be fixed pointwise by P_x. Hence, $P_x \leq P_y$. But since P is transitive, the groups P_x and P_y are conjugate, so they must be equal. ■

The following rather nice lemma was pointed out to me by David Witte, when he was trying to understand my original proof.

Lemma 4.5 *If a group G acts on a set X, and $x \in X$, then*

$$B = \{y \in X : G_x = G_y\}$$

is a G-block.

PROOF. Suppose $y \in B \bigcap gB$, for some $g \in G$. Since $y \in gB$, there exists $v \in B$ such that $y = gv$, and so

$$G_y = gG_vg^{-1} = gG_xg^{-1}.$$

Because $y \in B$, this means that $G_x = gG_xg^{-1}$. Suppose $z \in gB$. Then, as was true for y,

$$G_z = gG_xg^{-1} = G_x.$$

Hence $z \in B$, and since z was arbitrary, $gB \subseteq B$. Therefore $gB = B$, and B is a G-block. ■

Let K be a permutation group on a set X, with complete block systems based on blocks of two different sizes j and j', $j' < j$. Let X' be the set of blocks of size j' within a fixed block of size j. We examine those elements of K which fix each block of size j' setwise. If the permutation group formed by the action of these elements on the set X' is isomorphic to the group L, then we say that *K acts as L on the blocks of size j' within the blocks of size j.*

Lemma 4.6 *Suppose x and y are elements of the set $V(X)$ that are in different P-blocks of size p^i, and R acts as $\mathbf{Z}_p \times \mathbf{Z}_p$ on the blocks of size p^{i-1} within the blocks of size p^{i+1}, where $i \geq 1$. Then the P_x-orbit of y is not a subset of $B_{y,i-1}$.*

PROOF. We examine the group $P_{B_{x,i-1}}$, consisting of all automorphisms in P that fix $B_{x,i-1}$ setwise. (In particular, this contains P_x.) Now, suppose there is an element β of this group that moves y from $B_{y,i-1}$; that is, $\beta \in P_{B_{x,i-1}}$

and $\beta(y) \notin B_{y,i-1}$. Because $\beta(x) \in B_{x,i-1}$, there is some $\sigma \in Q_{B_{x,i-1}}$, such that $\sigma(\beta(x)) = x$; that is, $\sigma\beta \in P_x$. Because $Q_{B_{x,i-1}}$ fixes every block of size p^{i-1} setwise, we see that $\sigma\beta(y) \notin B_{y,i-1}$, which yields the result. So we may assume that every element of $P_{B_{x,i-1}}$ fixes $B_{y,i-1}$ setwise.

Let $\mathcal{B}$ be the set of blocks of size p^{i-1} that are contained in $B_{x,i+1}$. The preceding paragraph implies that $P_{B_{y,i-1}} = P_{B_{x,i-1}}$. Now by Lemma 4.5, the union of all blocks of size p^{i-1} which have the same setwise stabilizers is a P-block B containing both $B_{y,i-1}$ and $B_{x,i-1}$. But we know precisely what the P-blocks are, and since x and y are not in the same block of size p^i, B must contain $B_{x,i+1}$ at the very least. Hence every point in $\mathcal{B}$ has the same (setwise) stabilizer (namely $P_{B_{x,i-1}}$), so $\frac{P_{B_{x,i+1}}}{P_{B_{x,i-1}}}$ is a regular permutation group on the set $\mathcal{B}$.

Note, however, that the image of $Q_{B_{x,i+1}}$ in $\frac{P_{B_{x,i+1}}}{P_{B_{x,i-1}}}$ is cyclic, whereas the image of $R_{B_{x,i+1}}$ is isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$, by assumption. This means that $\frac{P_{B_{x,i+1}}}{P_{B_{x,i-1}}}$ contains two nonisomorphic transitive subgroups, which contradicts the regularity. ■

The proof of the next lemma is intricate, but not particularly deep. It is the only part of the proof of Theorem 1.1 that requires the assumption that p be odd.

Lemma 4.7 *Suppose x and y are elements of the set $V(X)$ that are in different P-blocks of size p^i. Then if the length of the P_x-orbit of y is at least p^j, then the entire block $B_{y,j}$ must be contained in this orbit.*

PROOF. The proof is by induction on j. The base case, $j = 0$, is trivial.

Now we suppose that the orbit has length at least p^j, where $1 \leq j$. By the induction hypothesis, the orbit must contain $B_{y,j-1}$. Since P_x is a p-group, and $B_{y,j}$ is a block of P and therefore of P_x, the intersection of the P_x-orbit of y with $B_{y,j}$ must have length a power of p, so the length is either p^{j-1} or p^j. If it is p^j then we are done, so we assume that it is p^{j-1}. Now, the rest of this orbit (which by assumption has length at least p^j) must consist of at least $p-1$ other blocks of size p^{j-1} within distinct blocks of size p^j. Since these are in the orbit of y, there is a $\beta \in P_x$ that takes y into one of these other blocks. Choose β in such a way that the size of the smallest block containing both y and $\beta(y)$ is minimized, while still being larger that p^j.

Let $B_{y,l}$ be the smallest P-block that contains both y and $\beta(y)$. Note that

$$l \quad \geq \quad j+1. \tag{1}$$

Let $\sigma \in Q$ be such that $\langle \sigma \rangle = Q$. Now, there exists a number a such that

$$\sigma^a(x) = y. \tag{2}$$

Also, since $\beta(y) \in B_{y,l}$, there must be some number b such that

$$\sigma^b \in Q_{B_{y,l}} \tag{3}$$

$$\text{and} \quad \sigma^b(y) = \beta(y). \tag{4}$$

$$\text{Hence,} \quad \sigma^{-a-b}\beta\sigma^a \in P_x. \tag{5}$$

(Recall also that $Q_{B_{y,l}}$ fixes every P-block of size p^l setwise.)

We will show (through long calculation) that

$$\beta^p(y) \in B_{\sigma^{pb}(y),l-2} \subseteq B_{y,l-1}.$$

Then the choice of β to minimize l will force

$$\beta^p(y) \in B_{y,j-1},$$

so we must have

$$B_{y,j-1} \subseteq B_{\sigma^{pb}(y),l-2}$$

since the intersection of these sets is nonempty and by (1). But this tells us that σ^{pb} fixes $B_{y,l-2}$ setwise, so $\sigma^{pb} \in Q_{B_{x,l-2}}$. Clearly then, $\sigma^b \in Q_{B_{x,l-1}}$. But this means that

$$\sigma^b(y) = \beta(y) \in B_{y,l-1},$$

contradicting the definition of l.

The only possibility remaining will be the truth of this lemma. Now to the calculations.

The smallest P-block containing both $x = \sigma^{-a}(y)$ and

$$\begin{aligned} \sigma^b(x) &= \sigma^{b-a}(y) \text{ (by (2))} \\ &= \sigma^{-a}\beta(y) \text{ (by (4))} \\ \text{must be} \quad \sigma^{-a}(B_{y,l}) &= B_{x,l}, \text{ (by (2))} \end{aligned}$$

so the P_x-orbit of $\sigma^b(x)$ is contained in $B_{\sigma^b(x),l-1}$. Thus there exist numbers c and d such that

$$\sigma^c, \sigma^d \in Q_{B_{x,l-1}} \tag{6}$$

$$\text{and} \quad \beta(\sigma^b(x)) = \sigma^c(\sigma^b(x)) \tag{7}$$

$$\text{and } \sigma^{-a-b}\beta\sigma^a(\sigma^b(x)) = \sigma^d(\sigma^b(x)) \text{ (using (5)).} \tag{8}$$

$$\text{Let} \quad \gamma = \sigma^{-b-c}\beta\sigma^b; \tag{9}$$

then $\gamma \in P_x$ (using (7)).

By (2) and (4), we have

$$\begin{aligned} \beta^2(y) &= \beta\sigma^{a+b}(x) \\ &= \sigma^{a+b}(\sigma^{-a-b}\beta\sigma^a)\sigma^b(x) \\ &= \sigma^{a+b+d+b}(x) \text{ (using (8))}. \qquad (10) \\ \text{Hence,} \quad \gamma(y) &= \sigma^{-b-c}\beta\sigma^b(y) \text{ (by (9))} \\ &= \sigma^{-b-c}\beta^2(y) \text{ (by (4))} \\ &= \sigma^{-b-c}\sigma^{a+2b+d}(x) \text{ (by (10))} \\ &= \sigma^{a+b-c+d}(x). \qquad (11) \end{aligned}$$

Now, by (6) and (11), we have that

$$\begin{aligned} \gamma(y) &\in B_{\sigma^{a+b}(x),l-1} \\ &= B_{\beta(y),l-1} \text{ (by (2), (4))}. \end{aligned}$$

Hence $B_{\gamma(y),l-1} = B_{\beta(y),l-1}$, so $\gamma^{-1}\beta(y)$ is in the block $B_{y,l-1}$. Our choice of β to minimize l forces $\gamma^{-1}\beta(y) \in B_{y,j-1}$. Hence we must have

$$\begin{aligned} \gamma(y) &\in B_{\beta(y),j-1} \qquad (12) \\ \text{and so} \quad \sigma^{a+b-c+d}(x) &\in B_{\sigma^{a+b}(x),j-1} \text{ (by (11), (2), (4))}, \\ \text{so} \quad \sigma^{d-c} &\in Q_{B_{x,j-1}}, \qquad (13) \\ \text{whence} \quad \beta^2(y) &= \sigma^{a+2b+d}(x) \text{ (by (10))} \\ &\in B_{\sigma^{a+2b+c}(x),j-1} \text{ (by (13))}. \qquad (14) \end{aligned}$$

By induction on k, we will now show that

$$\begin{aligned} \gamma^k(y) &\in B_{\beta^k(y),j-1} \qquad (15) \\ \text{and} \quad \beta^{k+1}(y) &\in B_{\sigma^{a+(k+1)b+\frac{k(k+1)}{2}c}(x),l-2}. \qquad (16) \end{aligned}$$

The base case for (15) is (12). We require two base cases for (16); the case for $k = 0$ is clear from (2) and (4), and the case $k = 1$ is clear from (14) and (1).

Since σ^b and $\sigma^c \in Q_{B_{x,l}}$ ((3), (5)) and $\sigma^{-a-b}\beta\sigma^a \in P_x$ (6), we must have some number e such that

$$\begin{aligned} \sigma^e &\in Q_{B_{x,l-1}} \qquad (17) \\ \text{and} \quad \sigma^{-a-b}\beta\sigma^a\sigma^{kb+\frac{k(k-1)}{2}c}(x) &= \sigma^e\sigma^{kb+\frac{k(k-1)}{2}c}(x). \qquad (18) \end{aligned}$$

Now, by induction,

$$\begin{aligned}\beta^{k+1}(y) &\in B_{\beta\sigma^{a+kb+\frac{k(k-1)}{2}c}(x),l-2} \text{ (by (16)),}\\ &= B_{\sigma^{a+b+e+kb+\frac{k(k-1)}{2}c}(x),l-2} \text{ (by (18))}\\ &= B_{\sigma^{a+(k+1)b+\frac{k(k-1)}{2}c+e}(x),l-2}. \qquad (19)\end{aligned}$$

Also, since $\sigma^c \in Q_{B_{x,l-1}}$ (6) and since $\beta \in P_x$, there must exist some number f such that

$$\begin{aligned}\sigma^f &\in Q_{B_{x,l-2}} \qquad (20)\\ \text{and} \quad \sigma^f\beta\sigma^{(1-k)c}(x) &= \sigma^{(1-k)c}(x).\\ \text{Let} \quad \psi &= \sigma^{(k-1)c+f}\beta\sigma^{(1-k)c}, \qquad (21)\end{aligned}$$

so $\psi \in P_x$.

By (9), we have

$$\begin{aligned}\gamma^k(y) &= \sigma^{-b-c}\beta\sigma^b\gamma^{k-1}(y)\\ &\in B_{\sigma^{-b-c}\beta\sigma^b\sigma^{a+(k-1)b+\frac{(k-1)(k-2)}{2}c}(x),l-2} \text{ (by (15), (16) and (1))}\\ &= B_{\sigma^{-b-c}\beta\sigma^{(1-k)c}\sigma^{a+kb+\frac{k(k-1)}{2}c}(x),l-2}\\ &= B_{\sigma^{-b-c}\beta\sigma^{(1-k)c}\beta^k(y),l-2} \text{ (by induction (16).)}\\ &= B_{\sigma^{-b-c-f+(1-k)c}\psi\beta^k(y),l-2} \text{ (by (21))}\\ &= B_{\sigma^{-b-kc}\psi\beta^k(y),l-2} \text{ (by (20)).} \qquad (22)\end{aligned}$$

Now we use (21) and the fact that σ^c and σ^f are in $Q_{B_{x,l-1}}$ ((6) and (20)) to note that

$$\psi\beta^k(y) \in B_{\beta^{k+1}(y),l-1}.$$

So the choice of β minimizing l again intervenes to force

$$\psi\beta^k(y) \in B_{\beta^{k+1}(y),j-1}. \qquad (23)$$

Using (1), (22) and (23), we see that

$$\begin{aligned}\gamma^k(y) &\in B_{\sigma^{-b-kc}\beta^{k+1}(y),l-2}\\ &= B_{\sigma^{-b-kc}\sigma^{a+(k+1)b+\frac{k(k-1)}{2}c+e}(x),l-2} \text{ (by (19))}\\ &= B_{\sigma^{a+kb+(\frac{k(k-1)}{2}-k)c+e}(x),l-2}. \qquad (24)\end{aligned}$$

Since σ^c and σ^e are in $Q_{B_{x,l-1}}$ ((6) and (17)), we see that the vertex

$$\sigma^{a+kb+(\frac{k(k-1)}{2}-k)c+e}(x) \in B_{\sigma^{a+kb+\frac{k(k-1)}{2}c}(x),l-1} = B_{\beta^k(y),l-1} \text{ (by (16))},$$

$$\text{so} \quad \gamma^k(y) \in B_{\beta^k(y),l-1}.$$

The choice of β to minimize l forces

$$\gamma^k(y) \quad \in \quad B_{\beta^k(y),j-1}, \tag{25}$$

the first of the desired inductive conclusions (15).

Combining (25), (24) and (1) with the inductive assumption from (16) that

$$\beta^k(y) \in B_{\sigma^{a+kb+\frac{k(k-1)}{2}c}(x),l-2},$$

we see that

$$\sigma^{-kc+e} \in Q_{B_{x,l-2}}. \tag{26}$$

Hence

$$\begin{aligned} \beta^{k+1}(y) \quad &\in \quad B_{\sigma^{a+(k+1)b+\frac{k(k-1)}{2}c+e}(x),l-2} \text{ (by (19))} \\ &= \quad B_{\sigma^{a+(k+1)b+\frac{k(k+1)}{2}c}(x),l-2} \text{ (by (26))}, \end{aligned}$$

which concludes the induction on k.

In particular, for $k = p-1$, we now have that

$$\begin{aligned} \beta^p(y) \quad &\in \quad B_{\sigma^{a+pb+\frac{p(p-1)}{2}c}(x),l-2} \text{ (by (16))} \\ &= \quad B_{\sigma^{pb+\frac{p(p-1)}{2}c}(y),l-2} \text{ (by (2))}. \end{aligned}$$

Because $\sigma^b \in Q_{B_{x,l}}$ (3) and $\sigma^c \in Q_{B_{x,l-1}}$ (6) and p divides $\frac{p(p-1)}{2}$ (this is the only place in the paper where the assumption of p being odd is necessary), we have

$$\sigma^{pb} \in Q_{B_{x,l-1}}$$

and

$$\sigma^{\frac{p(p-1)}{2}c} \in Q_{B_{x,l-2}}.$$

Hence,

$$\beta^p(y) \in B_{\sigma^{pb}(y),l-2} \subseteq B_{y,l-1},$$

and as mentioned earlier, this completes the proof. ■

Lemma 4.8 *Suppose x and y are elements of the set $V(X)$ that are in different P-blocks of size p^i, and R acts as $\mathbf{Z}_p \times \mathbf{Z}_p$ on the blocks of size p^{i-1} within the blocks of size p^{i+1}. Then the orbit of P_x containing y also contains all of $B_{y,j}$, for $0 \leq j \leq i$; in particular, $B_{y,i}$ is contained in the orbit.*

PROOF. The result is by induction on j. The base case of $j = 0$ is trivial.

In the induction hypothesis, we assume that $B_{y,j-1}$ is contained in the orbit. Since $j - 1 < i$, Lemma 4.6 tells us that the orbit is not contained within $B_{y,j-1}$, so there are other vertices in the orbit. Thus, the length of the orbit (being a power of p) must be at least p^j. Now Lemma 4.7 tells us that $B_{y,j}$ is contained in the orbit, as desired. ■

Fix a vertex $x \in V(X)$. A P-block B containing x is a *wreathed block* if for every $g, h \in P$, one of the following holds:

1. $gB = hB$
2. There is no arc from the vertices in gB to those in hB, or
3. There is an arc from every vertex in gB to every vertex in hB.

Corollary 4.9 *Suppose R does not act as $\mathbf{Z}_{p^{j-i}}$ on the blocks of size p^i within the blocks of size p^j, where $1 \leq i < j \leq n$. Then $B_{x,k}$ is a wreathed block, for some k such that $i < k < j$.*

PROOF. Since the action of R is not cyclic, there must be some i' and j' with $i \leq i' < j' \leq j$ such that $j' - i' = 2$, and R acts as $\mathbf{Z}_p \times \mathbf{Z}_p$ on the blocks of size $p^{i'}$ within the blocks of size $p^{j'}$. By Lemma 4.8 with $i = i' + 1$, if x is adjacent to a vertex $y \notin B_{x,i'+1}$, then x is adjacent to every vertex in $B_{y,i'+1}$. Hence $B_{x,k}$ is a wreathed block, where $k = i' + 1$. ■

Notice that since X is Cayley on the group G, the Sylow p-subgroup P must contain a subgroup R' which is conjugate to G in $\mathrm{Aut}(X)$. In Lemmata 4.6, 4.7 and 4.8 and Corollary 4.9, no special properties of R were employed; in fact, these lemmata continue to hold if R is replaced by R'.

Lemma 4.10 *There exist a chain of subgroups $G_1 \subset \ldots \subset G_{m-1}$ in G such that*

1. *$G_1, \frac{G_2}{G_1}, \ldots, \frac{G}{G_{m-1}}$ are cyclic groups;*
2. *$G_1 \times \frac{G_2}{G_1} \times \ldots \times \frac{G}{G_{m-1}} \leq_{po} H$;*

3. *For any vertices x and y in $V(X)$ with $y \notin G_i x$, if there is an arc from x to y in X then there is an arc from x to v for all vertices $v \in G_i y$.*

PROOF. Fix a vertex $x \in X$. List the wreathed P-blocks containing x in order:

$$\{x\} = B_0 \subset B_1 \subset \ldots \subset B_m = X.$$

For each i, there is a unique subgroup G_i of G with $B_i = G_i x$. Also, there is a unique subgroup H_i of H with $B_i = H_i x$.

By the definition of a wreathed block, condition (3) of the Lemma is immediate.

By Corollary 4.9 and the remark which followed it, the fact that there are no wreathed blocks between B_{i-1} and B_i implies that both $\frac{G_i}{G_{i-1}}$ and $\frac{H_i}{H_{i-1}}$ must be cyclic ($1 \leq i \leq m$), fulfilling condition (1).

Finally, since $\frac{G_i}{G_{i-1}}$ and $\frac{H_i}{H_{i-1}}$ have the same order $\frac{|B_i|}{|B_{i-1}|}$, they must be isomorphic groups. Since $G_0 = H_0$ is the identity, $G_m = G$ and $H_m = H$, we get

$$G_1 \times \frac{G_2}{G_1} \times \ldots \times \frac{G}{G_{m-1}} \cong H_1 \times \frac{H_2}{H_1} \times \ldots \times \frac{H}{H_{m-1}} \leq_{po} H.$$

■

Taking the case where x is the identity element of G, it is easy to see that this result is exactly condition (2) of the main result. This completes the proof of $1 \Rightarrow 2$. ■

5 What happens if $p = 2$?

As was noted earlier, only one lemma toward the proof of the main theorem required the assumption that p be odd. When p is even, I have not managed to prove a corresponding lemma, but neither have I found any counterexamples. Indeed, the following version of Theorem 1.1 is true when $p = 2$.

Theorem 5.1 *Let $X = X(G; S)$ be a Cayley digraph on an abelian group G of order 2^n. Then the following are equivalent:*

1. *The digraph X is isomorphic to a Cayley digraph on both $\mathbf{Z}_{p^n}$ and $H = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \ldots \times \mathbf{Z}_2$, where this group has order 2^n.*

2. *There exist a chain of subgroups $G_1 \subset \ldots \subset G_{m-1}$ in G such that*

(a) $G_1, \frac{G_2}{G_1}, \ldots, \frac{G}{G_{m-1}}$ *are cyclic groups;*

(b) $G_1 \times \frac{G_2}{G_1} \times \ldots \times \frac{G}{G_{m-1}} \leq_{po} H$;

(c) *For all* $s \in S \setminus G_i$, *we have* $sG_i \subseteq S$, *for* $i = 1, \ldots, m-1$. *(That is,* $S \setminus G_i$ *is a union of cosets of* G_i*.)*

3. *There exist Cayley digraphs* $U_1, \ldots, U_m$ *on cyclic p-groups* $H_1, \ldots, H_m$ *such that* $H_1 \times \ldots \times H_m \leq_{po} H$ *and* $X \cong U_m \wr \ldots \wr U_1$.

These in turn imply:

4. X *is isomorphic to Cayley digraphs on every abelian group of order* p^n.

The following lemma immediately gives us $(1 \Rightarrow 2)$ of Theorem 5.1.

Lemma 5.2 *Under the assumptions of (1) of Theorem 5.1, there are subgroups*

$$H_1 \subset \ldots \subset H_{n-1}$$

in G *such that* $|H_i| = p^i$ $(1 \leq i \leq n-1)$ *and for any vertices* x *and* y *in* X *with* $y \notin H_i x$, *if* x *and* y *are adjacent in* X *then* x *is adjacent to* v *for all vertices* $v \in H_i y$.

PROOF. Label the digraph X according to the group G. Then the P-block of size p^i containing the identity element of G is a subgroup of order p^i. This is true since adding any element of G in this block to every vertex is an automorphism of X that takes the identity element of G to another element in this same block, and hence fixes the block setwise. This means that the elements in this block form a closed set under addition, so are a subgroup. We call this subgroup H_i.

We will use induction, with trivial base case $n = 1$. Since the definitions of the subgroups H_i do not change in the inductive step, we can use the induction to assume that the result holds within the block $B_{x,n-1}$. Now we have two blocks of size 2^{n-1}, with x in one and y in the other. We will show that if x and y are adjacent in X, then every arc from $B_{x,n-1}$ to $B_{y,n-1}$ exists.

First, notice that since X is a Cayley digraph on $(\mathbf{Z}_2)^n$, a group of characteristic 2, the definition of a Cayley digraph tells us that for every arc from a to b coming from the element $b - a = b + a$ of S, there must be a corresponding arc from b to a coming from the element $a - b = a + b$ of S. So we really have a Cayley graph here. Notice also that any two vertices a

and b in $B_{y,n-1}$ have an even number of mutual neighbours in $B_{x,n-1}$. This is because for every vertex c in $B_{x,n-1}$ that is adjacent to a and b, the vertex $a+b-c = a+b+c$ is also adjacent to both a and b, and $a+b+c = c$ would imply $a+b = 0$ and hence $a = b$.

Consider X now as a Cayley graph on $\mathbf{Z}_{2^n}$, and label it accordingly. Since the graph is vertex-transitive, we may assume that 0 and x are the same vertex. If there are no edges from 0 to $B_{y,n-1}$, then it is not difficult to see that there are no edges between $B_{x,n-1}$ and $B_{y,n-1}$, and we are done. So we may assume that there is an edge between 0 and $y = m \equiv 1 \pmod 2$ without any loss of generality. Since X is a Cayley *graph*, the element $2^n - m$ is also in the symbol set S. Now as mentioned in the last paragraph, the vertices m and $-m$ must have an even number of mutual neighbours in $B_{x,n-1}$. Suppose $a \in B_{x,n-1}$ is adjacent to both m and $-m$. Then $-a$ is also adjacent to both m and $-m$. So the only way in which we can have an even number of mutual neighbours for m and $-m$, is if the vertex 2^{n-1} is adjacent to both m and $-m$. Thus, every vertex that is adjacent to 0 is also adjacent to 2^{n-1}.

Now, 2^{n-1} is the only other element in $B_{0,1}$, and we already know by our induction hypothesis that 0 and 2^{n-1} have precisely the same adjacencies within $B_{x,n-1}$. Since this is true for $B_{0,1}$, and the graph is vertex-transitive, the same must be true for each P-block of size 2. Hence we can form a new graph on p^{n-1} vertices, one corresponding to each of the P-blocks of size 2 in X, with an edge between two vertices if and only if all possible edges existed between the correspponding blocks in X. Now we use our induction hypothesis on this graph and carry the conclusion back to the original graph X, yielding the desired result. ■

Again, taking the case where x is the identity element of G in this lemma, yields condition (2) of Theorem 5.1.

6 Non-abelian groups

It is worthy of note that the only way in which the condition that G be abelian is used in this paper is to work with the richness of structure of the poset defined on abelian groups and to achieve condition (4) of the main theorem. So (using $H = G$ in the proof) we have the following theorem.

Theorem 6.1 *Let $X = X(G;S)$ be a Cayley digraph on a group G of order p^n, where p is an odd prime. Then the following are equivalent:*

1. *The digraph X is isomorphic to a Cayley digraph on $\mathbf{Z}_{p^n}$.*

2. *There exist a chain of subgroups* $G_1 < \ldots < G_{m-1}$ *in* G *such that*

   (a) $G_1, \frac{G_2}{G_1}, \ldots, \frac{G}{G_{m-1}}$ *are cyclic groups;*

   (b) *For all* $s \in S \setminus G_i$*, we have* $sG_i \subseteq S$*, for* $i = 1, \ldots, m-1$*. (That is,* $S \setminus G_i$ *is a union of cosets of* G_i*.)*

3. *There exist Cayley digraphs* $U_1, \ldots, U_m$ *on cyclic* p*-groups* $H_1, \ldots, H_m$ *such that there is some chain of subgroups* $G_1 < \ldots < G_{m-1}$ *in* G *with*

$$G_1 = H_1, \frac{G_2}{G_1} = H_2, \ldots, \frac{G}{G_{m-1}} = H_m$$

   and $X \cong U_m \wr \ldots \wr U_1$*.*

That is, a Cayley digraph on any group of prime power order can be represented as a Cayley digraph on the cyclic group of the same order if and only if the digraph is the wreath product of a sequence of Cayley digraphs on smaller cyclic groups.

7 Further extensions

In the general case where the digraph is on a number of vertices n that is not a prime power, less can be said immediately. First of all, if n is a product of distinct primes $p_1, \ldots, p_m$, then $\mathbf{Z}_{p_1} \times \ldots \times \mathbf{Z}_{p_m}$ is actually cyclic, and hence isomorphic to $\mathbf{Z}_n$. So any digraph which is a Cayley digraph on one group is necessarily Cayley on the other group.

Moreover, this is true if $n = n_1 n_2 \ldots n_m$ where n_i and n_j are coprime for every i and j with $1 \leq i < j \leq m$, and the groups under consideration are $\mathbf{Z}_n$ and $\mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_m}$.

If, on the other hand, p divides both n_i and n_j, and the digraph X is Cayley on both $\mathbf{Z}_n$ and $\mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_m}$, then we examine the Cayley digraph X' on those vertices of X that correspond to a Sylow p-subgroup of $\mathbf{Z}_n$. Due to the conjugacy of all Sylow p-subgroups of $\mathrm{Aut}(X)$, it is not hard to show that X' is also Cayley on a Sylow p-subgroup of $\mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_m}$. We can therefore use Theorem 1.1 of this paper to determine its form as a wreath product of smaller digraphs. The remainder of the structure of the digraph X is not so easy to determine in this case, and remains an interesting problem.

Another question that has been suggested is what happens in the case of digraphs that can be represented on two different abelian groups, neither of which is cyclic. The results in this paper rely heavily on properties of

the cyclic group, and I have not been able to make any significant progress toward answering this question.

Acknowledgements

I would like to thank my supervisor, Brian Alspach, who gave me several ideas as to where the partial results I achieved along the way might be generalized.

Both I and my readers are deeply indebted to David Witte, who battled his way through my original proofs of these results. He suggested several alternative proofs which have been incorporated into this, and make it far more reader-friendly than my original proofs!

Thanks also to my referees for their helpful suggestions to improve readability.

References

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

[2] M. Hall, *The Theory of Groups*, Macmillan, New York (1959).

[3] G. Sabidussi, On a class of fixed-point-free graphs, *Proc. Amer. Math. Soc.* 9 (1958), 800-804.

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

[5] H. Wielandt (trans. by R. Bercov), *Finite Permutation Groups*, Academic Press, New York (1964).