NORMAL CIRCULANT GRAPHS WITH NONCYCLIC REGULAR SUBGROUPS

DRAGAN MARUŠIČ AND JOY MORRIS

Abstract. We prove that any circulant graph of order n with connection set S such that n and the order of $\mathbb{Z}_n^*(S)$, the subgroup of $\mathbb{Z}_n^*$ that fixes S set-wise, are relatively prime, is also a Cayley graph on some noncyclic group, and show that the converse does not hold in general. In the special case of normal circulants whose order is not divisible by 4, we classify all such graphs that are also Cayley graphs of a noncyclic group, and show that the noncyclic group must be metacyclic, generated by two cyclic groups whose orders are relatively prime. We construct an infinite family of normal circulants whose order is divisible by 4 that are also normal Cayley graphs on dihedral and noncyclic abelian groups.

1. Introductory remarks

Much study over recent years has gone into the Cayley Isomorphism problem. One way of thinking of that problem, is as the question of when two Cayley graphs, each represented as a Cayley graph on the same group, can be isomorphic to one another. A significantly less-studied problem is the question of when two Cayley graphs, represented as Cayley graphs on two nonisomorphic groups, can be isomorphic to one another. In fact, the only results on the latter problem involve one of the groups being cyclic.

Joseph proved in 1995 [1] that a Cayley graph on the cyclic group $\mathbb{Z}_{p^2}$ can be represented as a Cayley graph on the elementary abelian group of order p^2 (where p is prime), if and only if the graph is a wreath product. Morris extended this result in [2] to show that a Cayley graph on the cyclic group $\mathbb{Z}_{p^n}$ can be represented as a Cayley graph on some noncyclic group of order p^n, if and only if the graph is a wreath product (in this case, p must be an odd prime, though one special case of the result is proven for $p = 2$).

Supported in part by the "Ministrstvo za šolstvo, znanost in šport Slovenije", research program no. P1-0285.

Supported in part by NSERC (National Science and Engineering Research Council of Canada).

In this paper, we first establish a condition that is sufficient in general (on any circulant graph) to guarantee that a circulant graph can also be represented as a Cayley graph on some noncyclic group; however, we also show that this condition is not necessary. We then restrict our attention to the case where the order of the circulant graph is not divisible by 4, require that the cyclic group be normal in the automorphism group of the graph, and arrive at a characterisation of when such graphs can be represented as a Cayley graph on some noncyclic group, and what the noncyclic group can be.

Throughout this paper graphs are simple and undirected. The symbol $\mathbb{Z}_n$, where n is an integer, will be used to denote the ring of integers modulo n as well as its (additive) cyclic group of order n.

Given a group G and a symmetric subset $S = S^{-1}$ of $G \setminus \{\mathrm{id}\}$, the *Cayley graph of G relative to S* has vertex set G and edges of the form $\{g, gs\}$, for all $g \in G$ and $s \in S$. A *circulant* is a Cayley graph of a cyclic group. More precisley, let n be a positive integer and $S \subseteq Z_n \setminus \{0\}$ satisfy $i \in S$ if and only if $n - i \in S$. The Cayley graph $Cir(n, S) = Cay(\mathbb{Z}_n, S)$ is called a *circulant* and the set S a *connection set* of $Cir(n, S)$. A Cayley graph on a group G is *normal* if its automorphism group contains a regular normal subgroup isomorphic to G. In particular, a circulant is *normal* if its automorphism group contains a cyclic regular normal subgroup. Note that this definition for a normal Cayley graph has emerged relatively recently in the literature. The term "normal Cayley graph" has also been used to mean a Cayley graph $Cay(G, S)$ in which S is a normal subset of G (so that the graph admits both right and left translation by G; this is not the sense in which this term is used in this paper, and neither definition implies the other.

For permutation group notation not defined in this paper, the reader is referred to [3].

2. The general sufficient condition

Given $Cir(n, S)$, let $\mathbb{Z}_n^*(S)$ denote the subgroup of $\mathbb{Z}_n^*$ that fixes S set-wise. Then we have the following result.

Theorem 2.1. *Let $X = Cir(n, S)$, and $\mathbb{Z}_n^*(S)$ be defined as above. Then if $\gcd(n, |\mathbb{Z}_n^*(S)|) > 1$, we have $X \cong Cay(G, S')$ for some $G \not\cong \mathbb{Z}_n$, and some $S' \subseteq G \setminus \{\mathrm{id}\}$.*

In fact, given any $G \cong \mathbb{Z}_p \ltimes \mathbb{Z}_{n/p}$, where p is any prime divisor of $\gcd(n, |\mathbb{Z}_n^*(S)|)$, there is some $S' \subseteq G \setminus \{\mathrm{id}\}$ such that $X \cong Cay(G, S')$.

Proof. Let p be any prime that divides both $|\mathbb{Z}_n^*(S)|$ and n. Then $\mathbb{Z}_n^*(S)$ has a subgroup of order p, say $a \in \mathbb{Z}_n^*(S)$ with $a^p \equiv 1 (\bmod n)$.

We claim that

$$G = \{g_{i,j} : g_{i,j}(x) = a^i x + \frac{a^i - 1}{a - 1} + jp, 0 \leq i < p, 0 \leq j < n/p\}$$

is a regular subgroup of $\mathrm{Aut}\,(X)$, and is isomorphic to $\mathbb{Z}_p \ltimes \mathbb{Z}_{n/p}$.

First, since $\mathbb{Z}_n \leq \mathrm{Aut}\,(X)$, if the map taking x to ax is in $\mathrm{Aut}\,(X)$, then each $g \in G$ will be in $\mathrm{Aut}\,(X)$. Now, if x and y are adjacent in X, then $y = x + s$ for some $s \in S$, so $ay = ax + as$ and since $a \in \mathbb{Z}_n^*(S)$, we have $as \in S$, so ay and ax are adjacent in X. It is straightforward to verify that the composition of any two elements of G is still in G. Thus, $G \leq \mathrm{Aut}\,(X)$.

Now we establish that G is regular. Clearly, since there are p choices for i and n/p choices for j, $|G| = n$. We show that G_0, the set of elements in G that fix 0, consists only of the identity. Suppose that $g = g_{i,j} \in G$ and g fixes 0. Then $\frac{a^i-1}{a-1} = -jp$ (in $\mathbb{Z}_n$). We will establish in the next paragraph that $0, \frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^p-1}{a-1}$ are all in different residue classes modulo p. Thus, $\frac{a^i-1}{a-1} = -jp$ forces $i = 0$, which in turn forces $j = 0$ as $j < n/p$, meaning g is the identity.

To establish our claim that $0, \frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^p-1}{a-1}$ are all in different residue classes modulo p, suppose that $\frac{a^r-1}{a-1} \equiv \frac{a^t-1}{a-1} (\bmod\, p)$, with $0 \leq r, t \leq p-1$, and that $t > r$. Then

$$\begin{aligned} \frac{a^r - 1}{a - 1} &\equiv \frac{a^t - 1}{a - 1} (\bmod\, p) \\ \Leftrightarrow a^{r-1} + \ldots + 1 &\equiv a^{t-1} + \ldots + a + 1 (\bmod\, p) \\ \Leftrightarrow a^{t-1} + a^{t-2} + \ldots + a^r &\equiv 0 (\bmod\, p) \\ \Leftrightarrow a^r(a^{t-r-1} + \ldots + a + 1) &\equiv 0 (\bmod\, p) \\ \Leftrightarrow \frac{a^{t-r} - 1}{a - 1} &\equiv 0 (\bmod\, p) \\ \Leftrightarrow t - r &\equiv 0 (\bmod\, p), \end{aligned}$$

a contradiction that establishes our claim, and thus completes the proof that G is regular.

Finally, we show that $G \cong \mathbb{Z}_p \ltimes \mathbb{Z}_{n/p}$, where $\mathbb{Z}_{n/p}$ is identified with the set $\{g_{0,j} \mid 0 \leq j < n/p\}$. We have

$$\begin{aligned} g_{i,j}^{-1} g_{0,\ell} g_{i,j}(x) &= g_{i,j}^{-1}(g_{i,j}(x) + \ell p) \\ &= g_{i,j}^{-1}(a^i x + \frac{a^i - 1}{a - 1} + (j + \ell)p) \\ &= x + a^{-i}\ell p \\ &= g_{0,a^{-i}\ell}(x) \end{aligned}$$

so $\mathbb{Z}_{n/p} \lhd G$.

It is easy to verify that G is nonabelian, so we must have $G \cong \mathbb{Z}_p \ltimes \mathbb{Z}_{n/p}$. □

Corollary 2.2. *Any circulant of even order is also a Cayley graph on the dihedral group of the same order.*

Proof. Since multiplication by -1 fixes S set-wise, $\{-1, 1\} \leq \mathbb{Z}_n^*(S)$, so $|\mathbb{Z}_n^*(S)|$ must be even. □

We note that the converse of Theorem 2.1 does not hold. The trivial example of this is the complete graph K_n, $n > 2$, where $\gcd(n, \phi(n)) = 1$ (so n must be odd and square-free). As n and $\phi(n)$ are coprime, the gcd of n with $|\mathbb{Z}_n^*(S)|$ must also be 1, but K_n can be written as a Cayley graph on any permutation group of degree n.

From this trivial example, more complicated examples can be built. For example, let m (odd) have the property that $\gcd(m, \phi(m)) = 1$, and let $n = mm'$, where m' is odd. Construct the circulant $Cay(n, S)$, where the elements of S are 1, -1, and all multiples of m' (so we have a number of copies of K_m, joined by a perfect matching). Then the only multipliers that fix S setwise are 1 and -1, and as n is odd, if the converse of the theorem were true, this graph shouldn't be Cayley on any other group. However, it is Cayley on the direct product of $\mathbb{Z}_{m'}$ with any permutation group of degree m.

3. A construction

We now construct circulants that are also Cayley graphs on more general metacyclic groups.

For any circulant $X = Cir(n, S)$ we have that S is a union of cosets of a subgroup of $\mathbb{Z}_n^*$, even if that subgroup be $\{1, -1\}$. Suppose $\gamma \in \mathrm{Aut}(X)$ is such that $\gamma(j) = j + 1$ for any j, where addition is performed modulo n.

For any element τ in $N(\langle\gamma\rangle)$ (that is, the normaliser of $\langle\gamma\rangle$ within the automorphism group of the graph), there must exist some r in $\mathbb{Z}_n^*$ such that τ has the form

$$\tau(x) = xr + \tau(0), \forall x.$$

Suppose $i \in S$. Then using the automorphism $\gamma^{-\tau(0)}\tau$, we see that ri must also be an element of S. So we must have $rS = S$.

Consider any other function τ' on X, defined by $\tau'(x) = xr + \tau'(0)$ with the same r. If $(i, j) \in E(X)$ then $j - i \in S$ so since $rS = S$, $rj - ri \in S$. Hence $(ir + \tau'(0), jr + \tau'(0)) \in E(X)$, and since this is the image of (i, j) under τ', we see that τ' must be an automorphism of X.

So the choice of $\tau(0)$ does not affect the structure of the graph. We will choose to look at the automorphisms defined by $\tau(0) = 1$, since there must be such an automorphism in any regular subgroup of the automorphism group of X.

We let $\mathcal{H}(S)$ be the largest subgroup of $\mathbb{Z}_n^*$ such that S may be written as a union of cosets of $\mathcal{H}(S)$, and let $r \in \mathcal{H}(S)$ have order k, dividing n. This ensures that τ is an automorphism of X. Notice that if $r = 1$ then $\tau = \gamma$. If some choice for r gives k such that k does not divide n, then since $\tau^x(0) = \frac{r^x-1}{r-1}$, the order of τ must be some multiple of k, which therefore does not divide n. Consequently, such a τ cannot be part of a regular subgroup of the automorphism group of X. If all choices for r except $r = 1$ give ks that do not divide n, then X can only be a Cayley graph on $\mathbb{Z}_n$. So we may assume that there is some $r \in \mathcal{H}(S)$ such that r has order $k > 1$ and $k|n$.

Now $\tau(x) = xr + 1$ for any x; so the order of τ is the least value y such that $\frac{r^y-1}{r-1} \equiv 0(\bmod n)$. Since k divides y, let $y = kt$. As above, if we cannot find some r such that kt divides n, X is not a Cayley graph on any group other than $\mathbb{Z}_n$. So we may assume that there is some $r \in \mathcal{H}(S)$ such that r has order $k > 1$ and $kt|n$.

We further assume that kt (the order of τ) is actually coprime with $\frac{n}{kt}$. It will be demonstrated in Theorem 4.3 that this condition is necessary for X to be a Cayley graph on some group other than $\mathbb{Z}_n$.

Now we take τ and γ^{kt}. Together, these generate a group of order n; calculations show that the group is transitive so must be regular. Furthermore, this group is clearly metacyclic.

Theorem 3.1. *Let $X = Cir(n, S)$ with $S = rS$ as above, the order of r in $\mathbb{Z}_n^*$ being k, the order of $\tau : x \to xr + 1$ being kt, $kt|n$, and $(kt, \frac{n}{kt}) = 1$. Then X is a circulant and a Cayley graph of the metacyclic group generated by γ^{kt} and τ, where $\tau(x) = xr + 1$ for any x.*

Proof. The proof is given in the construction above. □

Notice that not all of the graphs constructed above need be normal circulants. There is nothing in our construction to prevent the graph from having other automorphisms that do not normalise the cyclic group. However, some of them are normal circulants, and in the next section we will show that this construction yields all normal circulants that are Cayley graphs on any non-cyclic group.

4. Normal circulants, Cayley graphs on more than one group

In this section, we show that the graphs constructed in Section 3 of this paper are the only normal circulant graphs whose order is not divisible by 4, that are also Cayley graphs on some other group. We further show that the only regular normal subgroups in the automorphism groups of such graphs are either cyclic, or the metacyclic semidirect product of two cyclic groups whose orders are coprime. We finish the section with a construction of an infinite family of normal circulants whose order is divisible by 4 that are also normal Cayley graphs on dihedral and noncyclic abelian groups.

We require two lemmata before we can prove our main result.

Lemma 4.1. *Let G be a transitive group on a set X of cardinality p^i, where p is an odd prime and $i \geq 2$. Let $C = \langle \gamma \rangle$ be a regular cyclic normal subgroup of G and let R be a second regular subgroup of G. Let $B_0, B_1, \ldots, B_{p-1}$ be the blocks of G of length p^{i-1} formed by the orbits of γ^p, where $\gamma B_j = B_{j+1}$. If $\sigma \in R$ is such that $\sigma B_0 = B_1$, we must have $|\langle \sigma \rangle| > p$.*

Proof. Since R is regular on a set of cardinality p^i, R is a p-group. Hence $R \leq P(R)$, for some Sylow p-subgroup $P(R)$ of G. But since C is also a p-group and C is normal in G, we must have C in the intersection of all Sylow p-subgroups of G, so in particular, $C \leq P(R)$.

Since σ and γ are in the same p-group, and $\sigma^{-1}\gamma B_0 = B_0$, we must have $\sigma^{-1}\gamma B_j = B_j$ for all j, so that $\sigma B_j = B_{j+1}$ for all j.

Toward a contradiction, suppose that $|\langle \sigma \rangle| = p$. We will show that in this case, $\sigma\gamma\sigma^{-1} \notin \langle \gamma \rangle$, contradicting the normality of C.

We will actually perform all calculations using the quotient groups $C/\langle \gamma^{p^2} \rangle$ and $R/\langle \gamma^{p^2} \rangle$. Label the blocks formed by the orbits of γ^{p^2} by $B'_0, B'_1, \ldots, B'_{p^2-1}$, where $B'_k \subset B_j$ if and only if $k \equiv j \pmod{p}$, and the action of $\gamma/\langle \gamma^{p^2} \rangle$ takes B'_j to B'_{j+1}. Because $\sigma B_j = B_{j+1}$, we must have $\sigma B'_j = B'_k$ where $k \equiv j + 1 \pmod{p}$.

Since σ has order p by assumption, let one p-cycle in the disjoint cycle decomposition of σ consist of:

$$(B'_0\, B'_{1+x_1 p}\, B'_{2+x_2 p}\, \ldots\, B'_{p-1+x_{p-1} p}).$$

Now, σ and γ^p are two distinct elements of order p acting within a p-group on p^2 blocks, so they must commute and generate an elementary abelian group on p^2 elements. Since $\sigma \in R$, and R is regular, σ acts semiregularly on the set $\{B'_0, \ldots, B'_{p^2-1}\}$, and since σ commutes with γ^p in its action on these blocks, the other cycles in the disjoint cycle decomposition of σ have the form:

$$(B'_{kp}\, B'_{1+kp+x_1p}\, B'_{2+kp+x_2p}\, \dots\, B'_{p-1+kp+x_{p-1}p}).$$

Now we consider the conjugate $\sigma\gamma\sigma^{-1}$, in its action on these blocks. This is:

$$(B'_{1+x_1p}\, B'_{2+(x_2-x_1)p}\, B'_{3+(x_3-x_2)p}\, \dots\, B'_{p-1+(x_{p-1}-x_{p-2})p}\, B'_{-x_{p-1}p}\, B'_{1+p+x_1p}\, \dots).$$

In order for this to be a power of γ, we must have the differences between any two successive subscripts being equivalent modulo p^2.

First we deal with the special case $p = 3$. In this case, we have

$$1 + 3(x_2 - 2x_1) \equiv -3x_2 - 2 - 3(x_2 - x_1) \equiv 4 + 3x_1 + 3x_2 (\bmod 9),$$

that is,

$$x_2 - 2x_1 \equiv 2 + x_1 - 2x_2 \equiv 1 + x_1 + x_2 (\bmod 3),$$

or $x_2 + x_1 \equiv 2 + x_1 + x_2 \equiv 1 + x_1 + x_2 (\bmod 3)$, a clear contradiction that yields the desired conclusion.

So now we may assume $p > 3$. Thus, by the condition on differences between successive subscripts,

$$1+(x_2-2x_1)p \equiv 1+(x_3-2x_2+x_1)p \equiv 1+(x_j-2x_{j-1}+x_{j-2})p (\bmod p^2)$$

whenever $3 \le j \le p-1$. We show by induction that

$$x_j \equiv \frac{j(j-1)}{2}x_2 - j(j-2)x_1 (\bmod p)$$

for $3 \le j \le p-1$.

When $j = 3$, we have $x_3 \equiv 3x_2 - 3x_1 \equiv \frac{3\cdot 2}{2}x_2 - 3 \cdot 1x_1 (\bmod p)$, as desired. When $j = 4$, we have $x_4 \equiv 2x_3 - x_2 + x_2 - 2x_1 \equiv 6x_2 - 6x_1 - 2x_1 \equiv \frac{4\cdot 3}{2}x_2 - 4 \cdot 2x_1 (\bmod p)$, again as desired. These two cases form the basis for induction.

In general,

$$\begin{aligned} x_j &\equiv 2x_{j-1} - x_{j-2} + x_2 - 2x_1 \\ &\equiv 2(\frac{(j-1)(j-2)}{2}x_2 - (j-1)(j-3)x_1) \\ &\quad -\frac{(j-2)(j-3)}{2}x_2 + (j-2)(j-4)x_1 + x_2 - 2x_1 \\ &\equiv \frac{j(j-1)}{2}x_2 - j(j-2)x_1 (\bmod p). \end{aligned}$$

This completes the induction.

We also have:

$$1 + (x_2 - 2x_1)p \equiv 1 + p + x_1p + x_{p-1}p (\bmod p^2).$$

Thus,

$$x_2 - 2x_1 \equiv 1 + x_1 + x_{p-1} (\bmod p).$$

By our induction, we then have

$$\begin{aligned} x_2 - 2x_1 &\equiv 1 + x_1 + \frac{(p-1)(p-2)}{2} x_2 - (p-1)(p-3)x_1 (\bmod p) \\ &\equiv 1 + x_1 + x_2 - 3x_1 \\ &\equiv 1 + x_2 - 2x_1 (\bmod p). \end{aligned}$$

This is the desired contradiction, and we may therefore conclude $|\langle\sigma\rangle| \neq p$, as desired. □

Lemma 4.2. *Suppose that V is a set of cardinality n, and $C = \langle\gamma\rangle$ acts cyclically with order n on V. Further suppose that R is a group that acts regularly on V, normalises C, and contains semiregular elements σ of order s and τ of order t where s and $t = p^j$ are coprime, p prime. Also, τ normalises σ. Assume that $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$ where $|\sigma_i| = s_i = p_i^{e_i}$ and every p_i is a distinct prime. If σ_i does not commute with γ for any i, then τ commutes with σ.*

Proof. There exist integers c_i such that $\tau\sigma_i^{-1}\tau^{-1} = \sigma_i^{-c_i}$, with $c_i^t \equiv 1(\bmod s_i)$. We also have $\sigma_i^{-1}\gamma\sigma_i = \gamma^{x_i}$, $x_i^{s_i} \equiv 1(\bmod n)$ and $\tau^{-1}\gamma\tau = \gamma^y$, with $y^t \equiv 1(\bmod n)$.

Suppose that $c_i \not\equiv 1(\bmod s_i)$, that is, σ_i and τ do not commute. Then $\tau\sigma_i^{-1}\tau^{-1}\gamma\tau\sigma_i\tau^{-1} = \tau\sigma_i^{-1}\gamma^y\sigma_i\tau^{-1} = \tau\gamma^{yx_i}\tau^{-1} = \gamma^{x_i}$, but we also have this being $\sigma_i^{-c_i}\gamma\sigma_i^{c_i} = \gamma^{x_i^{c_i}}$. Hence, $x_i^{c_i} \equiv x_i(\bmod n)$. Together with $x_i^{s_i} \equiv 1(\bmod n)$ and assuming $x_i \neq 1$ since σ_i does not commute with γ, this forces $c_i - 1 \equiv kp_i^{z_i}(\bmod n)$ for some k with p_i and k coprime (note that $k \neq 0$, by the supposition that began this paragraph). Notice that $z_i < e_i$.

Now, since $c_i^t \equiv 1(\bmod s_i)$, we have $(kp_i^{z_i} + 1)^t \equiv 1(\bmod s_i)$, so $1 + t(kp_i^{z_i}) + ... + t(kp_i^{z_i})^{t-1} + (kp_i^{z_i})^t \equiv 1(\bmod s_i)$. We subtract 1 from both sides and divide through by $p_i^{z_i}$ to get:

$$tk + \frac{t(t-1)}{2}k^2p_i^{z_i} + \cdots + k^tp_i^{(t-1)z_i} \equiv 0(\bmod p_i^{e_i-z_i}).$$

Since $e_i - z_i \geq 1$, we must have $tk \equiv 0(\bmod p_i)$, contradicting previous assumptions.

So for every i, $c_i \equiv 1(\bmod s_i)$, that is, σ_i and τ commute, meaning that σ and τ commute. □

Theorem 4.3. *Let X be a normal circulant graph of order n, n not divisible by 4, which is also a Cayley graph on another (noncyclic) group R. Then X is in the family of graphs constructed in Section 3* *of this paper, and R is metacyclic, generated by two cyclic subgroups whose orders are relatively prime.*

Proof. Let C be the normal regular cyclic group in $G = \mathrm{Aut}\, X$, generated by γ. We may assume that $V(X) = \mathbb{Z}_n$ and that γ maps i to $i+1$. Let R be another (noncyclic) regular subgroup in G.

Let K_0 be the subgroup of C of order $q_1^{e_1} \dots q_x^{e_x}$ generated by the union of all subgroups of $R \cap C$ of order p^y, where p is prime and p^y is the largest power of p that divides n. That is, K_0 is the largest Hall subgroup of C that is contained in $R \cap C$. It may be that $K_0 = 1$, but certainly K_0 is cyclic since it is a subgroup of C. Let $n' = n/(q_1^{e_1} \dots q_x^{e_x})$, so n' is coprime with $q_1, \dots, q_x$.

Let $n' = p_1 p_2 \dots p_k$, where $p_1, \dots, p_k$ are all prime and in non-ascending order ($p_i \geq p_{i+1}$). Let $\mathcal{B}_i$ be the complete block system generated by the orbits of $\langle \gamma^{p_{i+1}p_{i+2}\cdots p_k} \rangle$, and $\mathcal{B}_0$ the complete block system whose blocks are the orbits of K_0. Let $\theta_i : G \to G/\mathcal{B}_i$, and let $K_i = \mathrm{Ker}\theta_\mathrm{i}$.

We begin by showing inductively that $R/(R \cap K_i)$ is regular on the blocks of $\mathcal{B}_i$ for every i. For the base case $i = 0$, this is clearly true. For $i > 0$, we will prove this by using the induction hypothesis to prove the additional result that $(R \cap K_i)/(R \cap K_{i-1}) = (C \cap K_i)/(C \cap K_{i-1})$. Inductively, we assume that $R/(R \cap K_{i-1})$ is regular. We know that $(C \cap K_i)/(C \cap K_{i-1}) \cong \mathbb{Z}_{p_i}$ is generated by $\overline{\gamma^{p_{i+1}\cdots p_k}}$ (where the bar indicates the action of this element on the blocks of $\mathcal{B}_{i-1}$). Showing that $\overline{\gamma^{p_{i+1}\cdots p_k}} \leq R/(R \cap K_{i-1})$ will complete the induction, because of the regularity of $R/(R \cap K_{i-1})$ and of R.

Suppose that $(C \cap K_i)/(C \cap K_{i-1}) \not\leq (R \cap K_i)/(R \cap K_{i-1})$, that is $R/(R \cap K_{i-1}) \cap (C \cap K_i)/(C \cap K_{i-1}) = 1$. For $B \in \mathcal{B}_i$ take the setwise stabiliser $R/(R \cap K_{i-1})_B = R/(R \cap K_{i-1}) \cap G/(K_{i-1})_B$ of B in $R/(R \cap K_{i-1})$. The regularity of $R/(R \cap K_{i-1})$ implies that $|R/(R \cap K_{i-1})_B| = p_i$. Let q be any prime dividing $p_{i+1} \dots p_k$ and different from p_i (if there is one). Consider the block system in $X/\mathcal{B}_{i-1}$ arising from the group $\langle \gamma^q \rangle$, of index q in C. Since $q < p_i$, it follows that $R/(R \cap K_{i-1})_B$ fixes each of of these blocks setwise. Doing this for all primes different from p_i, and subdividing the blocks in each case, we end up with a block system with blocks of cardinality p_i^j, for some j, where p_i^j is the largest power of p_i dividing $\frac{n}{p_1 \cdots p_{i-1}}$; with all of these blocks fixed setwise by $R/(R \cap K_{i-1})_B$. Now if $j = 1$, these blocks coincide with the blocks of $\mathcal{B}_i$, and so the semiregularity of $R/(R \cap K_{i-1})_B$ and the normality of $(C \cap K_i)/(C \cap K_{i-1})$ forces $R/(R \cap K_{i-1})_B = (C \cap K_i)/(C \cap K_{i-1})$. This yields the desired conclusion to the induction in this case.

So assume now that $j \geq 2$. Because n is not divisible by 4, we may assume $p_i > 2$. We let p_i^l be the largest size of successive blocks "inside" the blocks of length p_i^j, with the property that $R/(R \cap K_{i-1})_B$ moves p_i of them in a cycle. (In other words, blocks of length p_i^{l+1} are fixed by $R/(R \cap K_{i-1})_B$.) Take a block U of length p_i^{l+1} which is the union of p_i of these blocks of length p_i^l. Then U admits a cyclic action of a corresponding subgroup of $C/(C \cap K_{i-1})$, generated by the appropriate power of $\overline{\gamma}$. Furthermore we have the action of $R/(R \cap K_{i-1})_B$ which decomposes U into p_i^l cycles of length p_i. The corresponding element of order p_i does not normalise the p_i^{l+1}-cycle (from $C/(C \cap K_{i-1})$). This follows by Lemma 4.1.

This has shown that we must have $R/(R \cap K_i)$ regular on the blocks of $\mathcal{B}_i$ for all i, and furthermore $(R \cap K_{i+1})/(R \cap K_i) = (C \cap K_{i+1})/(C \cap K_i)$ for all i.

Now we show that if $p_i = p_{i+j} > 2$, then $(R \cap K_{i+j})/(R \cap K_{i-1})$ is cyclic. (Certainly if $p_k = 2$ then $(R \cap K_k)/(R \cap K_{k-1})$ is cyclic of order 2, as it acts on just 2 elements.) Toward a contradiction, suppose that $(R \cap K_{i+j'})/(R \cap K_i)$ is cyclic but $(R \cap K_{i+j'+1})/(R \cap K_i)$ is not, where $j' < j$. Notice that we must have $j' \geq 1$. Then $(R \cap K_{i+j'+1})/(R \cap K_{i+j'-1})$ contains an element of order p that permutes the blocks of $\mathcal{B}_{i+j'}$, as well as the element of order p that fixes each block of $\mathcal{B}_{i+j'}$ while permuting the blocks of $\mathcal{B}_{i+j'-1}$. These two elements contradict Lemma 4.1. So we have the desired conclusion.

Let $q_1, \dots q_{k'}$ be the distinct primes in the prime factorisation of n', in descending order, with $n' = q_1^{e_1} q_2^{e_2-e_1} \dots q_{k'}^{e_{k'}-e_{k'-1}}$.

We show by induction that $(R \cap K_{e_i})/(R \cap K_0)$ is cyclic for every i. It is clear from the argument above that $(R \cap K_{e_1})/(R \cap K_0)$ is cyclic. Inductively, we assume that $(R \cap K_{e_{i-1}})/(R \cap K_0)$ is cyclic. So $R \cap K_{e_{i-1}}$ contains an element σ such that $\overline{\sigma}$ (indicating the action of σ on the blocks of $\mathcal{B}_0$) generates the group $(R \cap K_{e_{i-1}})/(R \cap K_0)$. By the construction of K_0, we have n/n' is coprime with $q_1, \dots, q_{i-1}$, so we can take a power of σ if necessary to ensure that σ has order $q_1^{e_1} \dots q_{i-1}^{e_{i-1}}$. Now, $(R \cap K_{e_i})/(R \cap K_{e_{i-1}})$ is cyclic of order $q_i^{e_i}$, so we can similarly find an element τ in R such that $\overline{\tau}$ (indicating the action of τ on the blocks of $\mathcal{B}_{e_{i-1}}$) generates $(R \cap K_{e_i})/(R \cap K_{e_{i-1}})$ and τ has order $q_i^{e_i}$. Now we use Lemma 4.2. By the construction of K_0, none of the σ_i in the lemma can commute with γ (otherwise they would be in K_0, since $\langle \sigma_i, \gamma \rangle$ is a transitive and abelian group, and hence regular, so equal to $\langle \gamma \rangle$).

Furthermore, if τ does not normalise σ, we can reject it and give the name τ instead to one of its conjugates with the same qualities that we required of τ, that does normalise σ, as described in what follows. Since $\langle\sigma, K_0\rangle = R\cap K_{e_{i-1}}$ is normal in R, it follows that τ does normalise this group. Furthermore, since $\langle\sigma\rangle$ is a Hall subgroup of $\langle\sigma, K_0\rangle$ (because the orders of σ and K_0 are coprime), and any two Hall subgroups of $\langle\sigma, K_0\rangle$ are conjugate in $\langle\sigma, K_0\rangle$, we must have $\tau^{-1}\sigma\tau = \phi^{-1}\sigma\phi$ for some $\phi \in \langle\sigma, K_0\rangle$. The normaliser of $\langle\sigma\rangle$ in $\langle\sigma, K_0\rangle$ has index $|K_0|$, so the number of Hall subgroups of $\langle\sigma, K_0\rangle$, conjugate to $\langle\sigma\rangle$, must divide $|K_0|$. Since τ has order $q_i^{e_i}$, all orbits of Hall subgroups under conjugation by τ must have length some power of q_i. Since q_i and $|K_0|$ are coprime, there must be some of these Hall subgroups that are fixed setwise under conjugation by τ. If conjugation by τ fixes the subgroup generated by $\phi^{-1}\sigma\phi$, then conjugation by $\phi\tau\phi^{-1}$ fixes the subgroup generated by σ. Hence, as claimed, we can choose a τ with all of the qualities required in our original choice (qualities that are preserved under conjugation by ϕ), that also normalises σ.

So we conclude that σ and τ commute. Since the orders of σ and τ are coprime, $\langle\overline{\sigma\tau}\rangle$ (indicating the action on blocks of $\mathcal{B}_0$) generates $(R\cap K_{e_i})/(R\cap K_0)$, the desired inductive conclusion.

Hence, $R/(R\cap K_0)$ is cyclic, $R\cap K_0$ is cyclic, and R is not cyclic. Furthermore, the element $\sigma\tau$ in R generated in the final step of the above induction has order n' and normalises $R\cap K_0$. Thus, R is metacyclic. Since R contains an element τ' such that $\tau'(0) = 1$, and τ' normalises $\langle\gamma\rangle$, and τ' must permute the orbits of K_0 cyclically, we conclude that X is in the family of graphs we constructed in Section 3 of this paper, concluding the proof. □

It is worth noting that if 4 divides the order of the graph, the conclusion of this theorem is not true; on the contrary, many metacyclic groups that are not generated by cyclic subgroups whose orders are relatively prime may be regular subgroups of the automorphism group of the graph; in fact, they may even be normal regular subgroups of the automorphism group of the graph, as demonstrated in the following construction.

Let $n \geq 5$ be an integer and let $X(4n)$ denote the circulant $Cir(4n, S)$ where $S = \{1, 2, 2n-1, 2n+1, 4n-2, 4n-1\}$. We show that $X = X(4n)$ is a normal Cayley graph relative to a cyclic, a dihedral and a noncyclic abelian group isomorphic to $\mathbb{Z}_{2n} \times \mathbb{Z}_2$. To this end we first compute the automorphism group $G = \mathrm{Aut}\, X$.

Clearly the permutation γ mapping according to the rule $\gamma : i \to i+1$, for each $i \in \mathbb{Z}_{4n}$ and the permutation τ mapping according to the rule $\tau : i \to -i$ for each $i \in \mathbb{Z}_{4n}$ are automorphisms of X. In addition, it may be seen that the permutation α which fixes all even elements of

$\mathbb{Z}_{4n}$ and maps an odd i to $2n+i$ is also an automorphism of X. In fact, we claim that $G = \langle \gamma, \tau, \alpha \rangle$. To see this it suffices to check that the identity is the only automorphism fixing simultaneously 0 and 1, in other words, it suffices to see that the action of the stabilizer G_0 on the set of odd neighbors of 0 is faithful and regular. We omit the proof of this fact. (Also, note that the automorphism $\tau\alpha = \alpha\tau$ interchanges i and $-i$ for i even and interchanges i and $2n-i$ for i odd.)

We now identify the three regular subgroups inside G. They are the cyclic group $C = \langle \gamma \rangle$, the dihedral group $D = \langle \gamma^2, \tau\gamma \rangle$, and the nocyclic abelian group $\langle \gamma^2, \alpha\gamma^n \rangle$ which is isomorphic to $\mathbb{Z}_{2n} \times \mathbb{Z}_2$.

Observe that $\alpha\gamma\alpha = \gamma^{2n+1}$, so C is clearly normal in G.

To see that D is normal, note first that $\langle \gamma^2 \rangle$ is a normal subgroup in G. Moreover, $\tau(\tau\gamma)\tau = \gamma\tau = \tau\gamma^{-1} = (\tau\gamma)\gamma^2 \in D$. Next, $\alpha(\tau\gamma)\alpha = \tau\alpha\gamma\alpha = \tau\gamma^{2n+1} = (\tau\gamma)\gamma^{2n} \in D$. Finally, $\gamma^{-1}(\tau\gamma)\gamma = \tau\gamma^3 = (\tau\gamma)\gamma^2 \in D$.

As for the normality of A, we check the conjugates of $\alpha\gamma^n$. First, we have $\gamma^{-1}(\alpha\gamma^n)\gamma = \alpha\gamma^{2n-1}\gamma^n\gamma = \alpha\gamma^{3n} = \alpha\gamma^n\gamma^{2n} \in A$. Second, $\tau(\alpha\gamma^n)\tau = \alpha\tau\gamma^n\tau = \alpha\gamma^{-1} = \alpha\gamma^n\gamma^{2n} \in A$. And finally, $\alpha(\alpha\gamma^n)\alpha = \gamma^n\alpha = \alpha\gamma^{n(2n+1)} = \alpha\gamma^n\gamma^{2n^2} \in A$.

Acknowledgments. The authors would like to thank the anonymous referee for a helpful suggestion of a result to add to this paper.

References

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

[2] J. Morris, Isomorphic Cayley graphs on nonisomorphic groups, *J. Graph Theory*, **31** (1999), 345–362.

[3] H. Wielandt, “Finite Permutation Groups”, Academic Press, New York, 1964.

IMFM, Oddelek za matematiko, Univerza v Ljubljani, Jadranska 19, 61111 Ljubljana, Slovenia
E-mail address: dragan.marusic@uni-lj.si

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB. T1K 6R4, Canada
E-mail address: joy@cs.uleth.ca