Contributions to Discrete Mathematics

Volume 11, Number 1, Pages 1–6
ISSN 1715-0868

AUTOMORPHISMS OF CIRCULANTS THAT RESPECT PARTITIONS

JOY MORRIS

Abstract. In this paper, we begin by partitioning the edge (or arc) set of a circulant (di)graph according to which generator in the connection set leads to each edge. We then further refine the partition by subdividing any part that corresponds to an element of order less than n, according to which of the cycles generated by that element the edge is in. It is known that if the (di)graph is connected and has no multiple edges, then any automorphism that respects the first partition and fixes the vertex corresponding to the group identity must be an automorphism of the group (this is in fact true in the more general context of Cayley graphs). We show that automorphisms that respect the second partition and fix 0 must also respect the first partition, and so are again precisely the group automorphisms of $\mathbb{Z}_n$.

1. Introduction

In any Cayley digraph, there is a natural partition of the edge set according to the elements of the connection set that define them. If $\Gamma = \mathrm{Cay}(G; S)$ where $S = \{s_1, \dots, s_k\}$, then this natural partition is defined by

$$\mathcal{B} = \{\{(g, gs_i) : g \in G\} : 1 \leq i \leq k\}.$$

Now, observe that any $s_i \in S$ generates a subgroup of G. Let $G_{i,1}, G_{i,2}, \dots, G_{i,k_i}$ be the k_i distinct cosets of this subgroup where $G_{i,1} = \langle s_i \rangle$. Then we can form a partition $\mathcal{C}$ that is a refinement of $\mathcal{B}$, with

$$\mathcal{C} = \{\{(g, gs_i) : g \in G_{i,j}\} : 1 \leq j \leq k_i, 1 \leq i \leq k\}.$$

Notice that each set in $\mathcal{C}$ consists of precisely the edges of a cycle, all of whose edges are formed by a single element of S. In the case of a Cayley graph, we replace each of the ordered pairs above with the corresponding unordered pair, and eliminate any duplication that may result so that $\mathcal{B}$ and $\mathcal{C}$ are sets, not multi-sets.

Received by the editors September 27, 2012, and in revised form February 10, 2014.
2010 *Mathematics Subject Classification.* 05C25.
Key words and phrases. automorphism, circulant graph, Cayley graph.
This research was supported in part by the National Science and Engineering Research Council of Canada.

If β is an automorphism of a graph, we say that it *respects* a partition $\{A_1, \ldots, A_n\}$ of the edge set of that graph if

$$\{A_1, \ldots, A_n\} = \{\beta(A_1), \ldots, \beta(A_n)\}.$$

It is little more than an observation to prove that in a connected Cayley digraph, any automorphism that respects the partition $\mathcal{B}$ and fixes the vertex 1 is an automorphism of G. Because the digraph is connected, $\langle S\rangle = G$, and for an automorphism α that fixes the vertex 1 to respect the partition $\mathcal{B}$ means precisely that for any $s_i, s_j \in S$ we have $\alpha(s_i s_j) = \alpha(s_i)\alpha(s_j)$, and similarly for longer words from $\langle S\rangle$. In the case of graphs, the proof becomes more complicated since respecting the partition means only that $\alpha(s_i s_j)$ is one of $\alpha(s_i)\alpha(s_j)$, $\alpha(s_i)\alpha(s_j^{-1})$, $\alpha(s_i^{-1})\alpha(s_j)$, or $\alpha(s_i^{-1})\alpha(s_j^{-1})$. However, the proof of this for circulant graphs is a special case of our main theorem.

It is our main theorem that in the case of circulant graphs and digraphs (Cayley graphs on $\mathbb{Z}_n$), we can show that only group automorphisms of $\mathbb{Z}_n$ respect the partition $\mathcal{C}$ while fixing the vertex 0.

This question was suggested by Tomaž Pisanski. It arose in the context of studying the structure and automorphism groups of *GI*-graphs, a generalisation of both the class of generalised Petersen graphs and the Foster census *I*-graphs; see [1]. The question seemed to me to be of interest in its own right.

2. Main Theorem and Proof

A *Cayley digraph* $\mathrm{Cay}(G; S)$ for a group G and a subset $S \subset G$ with $1 \notin S$, is the digraph whose vertices correspond to the elements of G, with an arc from g to gs whenever $g \in G$ and $s \in S$. If S is closed under inversion, then we combine the arcs from g to gs and from gs to $gss^{-1} = g$ into a single undirected edge, and the resulting structure is a *Cayley graph.* A *circulant (di)graph* $\mathrm{Circ}(n; S)$ is a Cayley (di)graph on the group $G = \mathbb{Z}_n$.

We assume that $\Gamma = \mathrm{Circ}(n; S)$ is fixed, with $S = \{s_1, \ldots, s_c\}$. We introduce some notation that will be useful in our proof: For any k, we will use S_k to denote the group $\langle s_1, \ldots, s_k\rangle$.

We begin with some lemmas. Notice that since the circulant graph is defined on a cyclic group, we will be using additive notation for this group.

Lemma 2.1. *Let $\alpha \in \mathrm{Aut}(\Gamma)$ respect $\mathcal{C}$ and fix the vertex labelled 0. Suppose $s, s' \in S$ and $\alpha(s) \equiv js \pmod{n_1}$, where $n = n_1 n_2$, $\gcd(n_1, n_2) = 1$, and $\langle n_2\rangle \leq \langle s\rangle$. Then $\alpha(s') \equiv js' \pmod{n_1}$.*

Proof. Let m be given such that $mn_2 \equiv 1 \pmod{n_1}$ so $\gcd(m, n_1) = 1$; such an m exists since $\gcd(n_1, n_2) = 1$. Since α respects $\mathcal{C}$, we have $\alpha(as) \equiv ajs \pmod{n_1}$, for any $a \in \mathbb{Z}$. In particular,

$$\alpha(amn_2 s) \equiv amn_2 js \pmod{n_1} \equiv ajs \pmod{n_1}$$

for any integer a.

Since $\langle n_2\rangle \le \langle s\rangle$, there is some t such that $st = n_2$, and so st has order n_1 in $\mathbb{Z}_n$. By the definition of m, we see that $mn_2st \equiv st \pmod{n_1}$, and hence has order n_1 in $\mathbb{Z}_n$. Thus every element of $\langle n_2\rangle$ can be written as a multiple of mn_2s.

Consider $\alpha(mn_2s')$. Clearly $mn_2s' \in \langle n_2\rangle$, so $mn_2s' = xmn_2s$ for some integer x. Now

$$\alpha(mn_2s') = \alpha(xmn_2s) \equiv xmn_2js \pmod{n_1}$$

by the conclusion of the first paragraph of this proof. Furthermore, this is congruent to mn_2js'. Since α respects $\mathcal{C}$, we know that

$$mn_2\alpha(s') = \alpha(mn_2s') \equiv mn_2js' \pmod{n_1}.$$

Because m and n_2 are coprime to n_1, this implies that $\alpha(s') \equiv js' \pmod{n_1}$, as desired. □

The next lemma follows from the first. We will be using notation that was introduced by Godsil in [2] and has become standard: $\mathrm{Aut}(G;S)$ denotes the automorphisms of the group G that fix S setwise, where $S \subseteq G$.

Lemma 2.2. *Assume Γ is connected. Let $\alpha \in \mathrm{Aut}(\Gamma)$ respect $\mathcal{C}$ and fix the vertex labelled 0. Then there is some $\beta \in \mathrm{Aut}(\mathbb{Z}_n;S)$ such that $\beta\alpha$ fixes the vertex as for every $a \in \mathbb{Z}$ and every $s \in S$.*

Proof. Let $n = p_1^{e_1}\dots p_r^{e_r}$, where $p_1,\dots,p_r$ are distinct primes. Now, since Γ is connected, for any p_i there is some $s_i \in S$ such that $p_i \nmid s_i$ and $\langle n/p_i^{e_i}\rangle \le \langle s_i\rangle$. Let j_i be given such that $\alpha(s_i) \equiv j_is_i \pmod{p_i^{e_i}}$. Notice that $j_i \not\equiv 0 \pmod{p_i}$ since α respecting $\mathcal{C}$ implies that both s_i and $\alpha(s_i)$ have the same order in $\mathbb{Z}_n$. Thus the conditions of Lemma 2.1 are satisfied and we conclude that for any $s \in S$ we have $\alpha(s) \equiv j_is \pmod{p_i^{e_i}}$.

Let j be an integer such that $j \equiv j_i \pmod{p_i^{e_i}}$ for every $1 \le i \le r$, and $1 \le j \le n-1$; such a j exists by the Chinese Remainder Theorem. Then for every $s \in S$, we have $\alpha(s) = js$, since this is the only value that satisfies all of the congruences. Furthermore, since α respects $\mathcal{C}$, for every $a \in \mathbb{Z}$ and every $s \in S$ we have that $\alpha(as) = ajs$.

Now let $\beta \in \mathrm{Aut}(\mathbb{Z}_n)$ be the automorphism that corresponds to multiplication by j^{-1}. Note that since $j \not\equiv 0 \pmod{p_i}$ for any index i, $j \in \mathbb{Z}_n^*$ has an inverse, and multiplication by this inverse is an automorphism of $\mathbb{Z}_n$. Since α is an automorphism of Γ and $\alpha(s) = js$ for every $s \in S$, we see that multiplication by j fixes S setwise, so $\beta \in \mathrm{Aut}(Z_n;S)$. Clearly $\beta\alpha$ fixes as for every $a \in \mathbb{Z}$ and every $s \in S$. □

The next lemma is an easy consequence of the definition of respecting $\mathcal{C}$, but is very useful.

Lemma 2.3. *Let $G = \langle S'\rangle$ for some $S' \subseteq S$ and let $\alpha \in \mathrm{Aut}(\Gamma)$ respect $\mathcal{C}$. Then for any $x \in \mathbb{Z}_n$, $\alpha(x+G)$ is a coset of G.*

Proof. For any $s \in S$ we have that x and $x+s$ are together in a cycle C of length $|s|$. Since α respects $\mathcal{C}$, $\alpha(C)$ is also a cycle of length $|s|$. Moreover, since $\mathbb{Z}_n$ has a unique subgroup of order $|s|$, $\alpha(C)$ must be a coset of this subgroup. Suppose $\alpha(x) = y$. Then for every $s \in S'$, $\alpha(C) = y + \langle s \rangle$, giving us that $\alpha(x+G) = y+G$. □

We can use Lemma 2.2 to assume that many of the vertices of Γ are fixed by α. Specifically we can assume vertices of the form as, where $a \in \mathbb{Z}$ and $s \in S$, are fixed. In our next lemma, we show that if some vertices are known to be fixed by a graph automorphism that respects $\mathcal{C}$, this will force other vertices to be fixed as well. This lemma is technical, but is the very core of the proof of our main theorem.

Lemma 2.4. *Let $G = \langle S' \rangle$ for some $S' \subseteq S$. Furthermore, let $|G| = n'$, let $s \in S$ with $|s| = r$, and let $d = \gcd(n', r)$. Suppose that $\alpha \in \mathrm{Aut}(\Gamma)$ fixes every vertex of some set T, where $G \subseteq T \subseteq G' = \langle G, s \rangle$, and T is a union of cosets of $\langle n/d \rangle$. If $x, x+s', x+s \in T$ with $s' \in S'$, then α fixes $x+s+s'$.*

Proof. By assumption, α fixes x, $x+s$, and $x+s'$. In G', every coset of G contains at least one vertex of $\langle s \rangle$. Since this vertex is fixed by α, by Lemma 2.3 we have that every coset of G in G' is fixed setwise by α. Similarly, every coset of $\langle s \rangle$ in G' contains at least one vertex of G, and hence is fixed setwise by α. Hence every intersection of a coset of G with a coset of $\langle s \rangle$ is fixed (setwise) by α, that is, every coset of $\langle n/d \rangle$ in G' is fixed setwise by α. If $d = 1$ then these cosets are all singletons, one of which is $x+s+s'$, and we are done. We therefore assume $d > 1$.

Since the coset of $\langle n/d \rangle$ that contains $x+s+s'$ is fixed setwise by α, we must have

$$\alpha(x+s+s') = x+s+s'+z(n/d)$$

for some $z < d$. If $z = 0$ then we are done, so suppose $0 < z < d$.

Choose p prime and $a \in \mathbb{Z}$ such that $p^a \mid d$ but $p^a \nmid z$; such a p and a exist because $0 < z < d$. Since α respects $\mathcal{C}$, fixes $x+s'$, and takes $x+s'+s$ to $x+s'+s+z(n/d)$, we must have

$$\alpha(x+s'+bs) = x+s'+b(s+z(n/d))$$

for any integer b. In particular, when $b = r/d$, we get

$$\alpha(x+s'+(r/d)s) = x+s'+r/d(s+z(n/d)).$$

Now, since $|s| = r$ in $\mathbb{Z}_n$, we must have $s = \ell(n/r)$ for some ℓ coprime to n. Thus $(r/d)s = (r/d)\ell(n/r) = \ell(n/d)$. Since $x+s' \in T$ and T is a union of cosets of $\langle n/d \rangle$,we have that $x+s'+(r/d)s \in T$, and so by assumption α fixes $x+s'+(r/d)s$. Hence $(r/d)z(n/d) \equiv 0 \pmod{n}$, implying that we must have $d \mid z(r/d)$. In particular, p^a divides $z(r/d)$, and since $p^a \nmid z$, this means $p \mid r/d$.

Similarly, since α respects $\mathcal{C}$, fixes $x+s$, and takes $x+s+s'$ to $x+s+s'+z(n/d)$, we must have that

$$\alpha(x+s+bs') = x+s+b(s'+z(n/d))$$

for any integer b. In particular, when $b = n'/d$, we get

$$\alpha(x + s + (n'/d)s') = x + s + (n'/d)(x' + z(n/d)).$$

Since $|G| = n'$ is cyclic and $s' \in G$, we have $s' = k(n/n')$ for some k. Thus $(n'/d)s' = (n'/d)k(n/n') = k(n/d)$. Because $x + s \in T$ and T is a union of cosets of $\langle n/d\rangle$, this shows that $x + s + (n'/d)s' \in T$, so by assumption α fixes $x + s + (n'/d)s'$. Hence $(n'/d)z(n/d) \equiv 0 \pmod{n}$, giving us that we must have $d \mid z(n'/d)$. In particular, p^a divides $z(n'/d)$, and since $p^a \nmid z$, this means $p \mid n'/d$.

This contradicts the definition of $d = \gcd(n', r)$. Thus we must have $z = 0$, and hence $\alpha(x + s + s') = x + s + s'$. □

We are now ready to prove our main theorem.

Theorem 2.5. *Let $\Gamma = \mathrm{Circ}(n; S)$ be a connected circulant graph. Let $\alpha \in \mathrm{Aut}(\Gamma)$ fix the vertex 0 and respect the partition $\mathcal{C}$, so for any $C \in \mathcal{C}$, $\alpha(C) \in \mathcal{C}$. Then $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.*

Proof. By Lemma 2.2, after replacing α by $\beta\alpha$ if necessary, we may assume that α fixes as for every $a \in \mathbb{Z}$ and every $s \in S$. We will show that α in fact fixes every vertex of Γ, so $\alpha = 1 \in \mathrm{Aut}(\mathbb{Z}_n)$.

We proceed with a nested induction argument in order to prove that every vertex of Γ is fixed by α. In the outer induction we will prove that for each i, every vertex of S_i is fixed by α. For our base case, we know that every vertex of $S_1 = \langle s_1\rangle$ is fixed by α, as every vertex of $\langle s\rangle$ is fixed by α for every $s \in S$. Inductively, assume that every vertex of S_k is fixed by α. We will deduce that every vertex of S_{k+1} is fixed by α.

In order to continue with the induction define $T_0 = S_k \cup \langle s_{k+1}\rangle$, and for $m \geq 1$,

$$T_m = T_{m-1} \cup \{s \in S_{k+1} : \exists y, 1 \leq y \leq k, \text{ and } s - s_{k+1}, s - s_y \in T_{m-1}\}.$$

It is not hard to see that every element of S_{k+1} will be in T_m for some m. Our inner inductive argument will be to show that for each i, every vertex in T_i is fixed. Observe that since S_k is fixed pointwise by α by our outer inductive hypothesis, and since every vertex of $\langle s_{k+1}\rangle$ is fixed by α, every vertex of T_0 is also fixed by α. This is the base case for our inner induction.

Suppose that $x' \in T_m$. If $x' \in T_{m-1}$ then by our inductive hypothesis, the coset of $\langle n/d\rangle$ that contains x' is in T_{m-1}. If $x' \notin T_{m-1}$ then $x' - s_{k+1} \in T_{m-1}$ and there is some $1 \leq y \leq k$ such that $x' - s_y \in T_{m-1}$. But since T_{m-1} is a union of cosets of $\langle n/d\rangle$, this means that $x' - s_{k+1} + \langle n/d\rangle \subseteq T_{m-1}$ and $x' - s_y + \langle n/d\rangle \subseteq T_{m-1}$, implying that $x' + \langle n/d\rangle \subseteq T_m$, as was desired.

Now we proceed with our main inner inductive argument, to show that α fixes every point of S_{k+1}. Suppose that every vertex in T_m is fixed by α and let x' be an arbitrary vertex of T_{m+1}. If $x' \in T_m$ then α fixes x' by hypothesis and we are done. Thus, by the definition of T_{m+1}, we have $x' - s_y \in T_m$ for some $1 \leq y \leq k$, and inductively that either $x' - s_y - s_{k+1} \in T_{m_1}$ for some $m_1 \leq m-1$, or $x' - s_y \in T_0$. If $x' - s_y \in \langle s_{k+1}\rangle$ then $x' - s_y - s_{k+1} \in T_0 \subset T_m$, while if $x' - s_y \in S_k$ then $x' \in S_k$ is fixed by α and we are done. So we may assume that $x = x' - s_y - s_{k+1} \in T_m$, as well as $x + s_{k+1} = x' - s_y \in T_m$ and $x + s_y = x' - s_{k+1} \in T_m$.

We appeal to Lemma 2.4, with $G = S_k$, $s = s_{k+1}$, and $T = T_m$. Since all of the conditions of the lemma are satisfied, we conclude that α fixes $x + s_y + s_{k+1} = x'$. Thus every vertex of T_{m+1} is fixed by α. This completes the inner induction, allowing us to conclude that every vertex of S_{k+1} is fixed by α, which completes the outer induction and hence completes the proof. $\square$

Acknowledgements

I am very much indebted to Tomaž Pisanski for suggesting this question.

References

1. M. Conder, T. Pisanski, and A. Žitnik, *GI-graphs: a new class of graphs with many symmetries*, J. Algebraic Combin. **40** (2014), no. 1, 209–231.
2. C. Godsil, *On the full automorphism group of a graph*, Combinatorica **1** (1981), no. 3, 243–256.

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