AUTOMORPHISMS OF CIRCULANTS THAT RESPECT PARTITIONS

JOY MORRIS

Abstract. In this paper, we begin by partitioning the edges (or arcs) 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, so are again precisely the group automorphisms of $\mathbb{Z}_n$.

1. Introduction

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

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

Now, any $s_i \in S$ generates a subgroup of G. Let $G_{i,1}, G_{i,2}, \ldots, G_{i,k_i}$ be the k_i distinct cosets of this subgroup (and $G_{i,1} = \langle s_i \rangle$). 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 $\mathcal{B}$ and $\mathcal{C}$ are sets, not multi-sets).

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 to respect the partition $\mathcal{B}$ means precisely that for any $s_i, s_j \in S$ we have $\alpha(s_i s_j) = \alpha(s_i)\alpha(s_j)$. Similarly for longer words from $\langle S \rangle$. In the case of graphs, the proof becomes more complicated since preserving 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.

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.

It is our main theorem that in the case of circulant graphs and digraphs (Cayley graphs on $\mathbb{Z}_n$), we can similarly 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 introduce some notation that will be useful in our proof. For this notation, we assume that $\mathrm{Circ}(n; S)$ is fixed, with $S = \langle s_1, \dots, s_c\rangle$. For any k, we will use S_k to denote $\langle s_1, \dots, s_k\rangle$, and $n_k = |S_k|$. Finally, for any integer r that divides n, we will use r' to denote the largest divisor of n for which every prime divisor of r' also divides r. In other words, if $r = p_1^{e_1} \dots p_\ell^{e_\ell}$, and for each $1 \leq i \leq \ell$ we have $p_i^{a_i}$ is the greatest power of p_i that divides n, then $r' = p_1^{a_1} \dots p_\ell^{a_\ell}$. We will then have $\gcd(r', n/r') = 1$.

We present our main theorem. Notice that since the circulant graph is defined on a cyclic group, we will be using additive notation for this group.

Theorem 2.1. *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. We will show that there exist $\alpha_1, \dots, \alpha_t \in \mathrm{Aut}(\mathbb{Z}_n)$ such that $\alpha_t \dots \alpha_1\alpha = 1$. The result follows. For simplicity, we will use the notation $\beta_k = \alpha_k \dots \alpha_1\alpha$ for any k.

We proceed inductively. Assume that β_k fixes every vertex in S_k. We aim to show that there exists $\alpha_{k+1} \in \mathrm{Aut}(\mathbb{Z}_n)$ such that $\alpha_{k+1}\beta_k$ fixes every vertex in S_{k+1}. This will complete the proof.

In our base case, $k = 0$ and we require only that α fixes 0; this assumption is given in our statement.

We first dispose of a trivial case. If $s_{k+1} \in S_k$, we let $\alpha_{k+1} = 1$. Since β_k fixes every vertex in $S_k = S_{k+1}$, we have $\alpha_{k+1}\beta_k = \beta_k$ fixes every vertex in S_{k+1}, as required.

Let $\gcd(n_k, |s_{k+1}|) = d \geq 1$, and let $|s_{k+1}| = r$. The first step in our proof will be to consider the image of s_{k+1} under β_k. We will show that $\beta_k(s_{k+1}) = s_i = js_{k+1}$ where $i \geq k+1$, $\gcd(j, r) = 1$, and $j \equiv 1 \pmod{d}$.

By our induction hypothesis, β_k fixes every point of $S_k = \langle n/n_k\rangle$; in particular, it fixes 0, so there must be some $i \geq k+1$ such that $\beta_k(s_{k+1}) = s_i$. In fact, since β_k respects $\mathcal{C}$, we must have $\beta_k(as_{k+1}) = as_i$ for any a. In particular, $|s_i| = r$, so $s_i \in \langle s_{k+1}\rangle = \langle n/r\rangle$. Choose j such that $s_i = js_{k+1}$ and ℓ such that $s_{k+1} = \ell n/r$. Notice that $\gcd(r, j) = \gcd(r, \ell) = 1$ since each of s_i, s_{k+1}, and n/r generates the subgroup of order r in $\mathbb{Z}_n$.

We now show that $j \equiv 1 \pmod{d}$. Notice that for any a,

$$a(r/d)s_{k+1} = a\ell(r/d)(n/r) \in \langle n/d\rangle \leq \langle n/n_k\rangle = S_k,$$

so is fixed by β_k. Hence

$$\beta_k(a(r/d)\ell(n/r)) = a(r/d)s_i = a(r/d)j\ell(n/r) = a(r/d)\ell(n/r).$$

Since $\gcd(\ell, r) = 1$, we can choose a such that $a\ell \equiv 1 \pmod{r}$, so $a\ell(n/r) \equiv n/r \pmod{n}$. Thus, this gives $j(n/d) = n/d$. Since our vertices are labelled modulo n, this means that $j \equiv 1 \pmod{d}$, as claimed, completing the first step.

For the second step in our proof, we will find an automorphism α_{k+1} of $\mathbb{Z}_n$ such that β_{k+1} fixes every point of S_k and every point of $\langle s_{k+1}\rangle$.

Since $\gcd(j, r) = 1$, there is a multiplicative inverse for j in $\mathbb{Z}_r$; call this element j^{-1}. Since $j \equiv 1 \pmod{d}$, we also have $j^{-1} \equiv 1 \pmod{d}$. Since $\gcd(n_k, r) = d$ and each of r, $j^{-1} - 1$ and n_k is a multiple of d, we can find some t such that $tr \equiv 1 - j^{-1} \pmod{n_k}$. Let $x = tr + j^{-1}$. By our choice of t, we have $x \equiv 1 \pmod{n_k}$; also, $xj = trj + 1 \equiv 1 \pmod{r}$. Now, $\gcd(n'_{k+1}, n/n'_{k+1}) = 1$, and $\mathbb{Z}_n \cong \mathbb{Z}_{n'_{k+1}} \times \mathbb{Z}_{n/n'_{k+1}}$. For simplicity, we will abuse notation by writing elements in $\mathbb{Z}_n$ as equal to their images in $\mathbb{Z}_{n'_{k+1}} \times \mathbb{Z}_{n/n'_{k+1}}$ under this isomorphism. In this representation of $\mathbb{Z}_n$, we can see that for any $s \in S_{k+1} = \langle n/n_{k+1}\rangle$, we have $|s|$ divides n_{k+1}, so $\gcd(|s|, n/n'_{k+1}) = 1$. Hence we must have $s = (\hat{s}, 0)$ for some $\hat{s} \in \mathbb{Z}_{n'_{k+1}}$. Let α_{k+1} be the automorphism of $\mathbb{Z}_n$ determined by multiplying every element of $\mathbb{Z}_{n'_{k+1}} \times \mathbb{Z}_{n/n'_{k+1}}$ by $(x, 1)$ (component-wise). Since $x \equiv 1 \pmod{n_k}$ and $xj \equiv 1 \pmod{r}$ (which implies that $\gcd(x, r) = 1$), we have $\gcd(x, n_{k+1}) = 1$, so $\gcd(x, n'_{k+1}) = 1$, and this is indeed an automorphism of $\mathbb{Z}_n$.

We claim that $\beta_{k+1} = \alpha_{k+1}\beta_k$ fixes every point of $S_k = \langle n/n_k\rangle$ and every point of $\langle s_{k+1}\rangle = \langle n/r\rangle$. Let $\hat{s}_{k+1}$ be such that $s_{k+1} = (\hat{s}_{k+1}, 0)$ under the isomorphism discussed in the previous paragraph. We have

$$\begin{aligned}
\alpha_{k+1}\beta_k(as_{k+1}) = \alpha_{k+1}(as_i) &= a\alpha_{k+1}(s_i)\\
&= a\alpha_{k+1}((j\hat{s}_{k+1}, 0))\\
&= a(xj\hat{s}_{k+1}, 0)\\
&= axjs_{k+1}\\
&= a\ell xj(n/r).
\end{aligned}$$

Since $xj \equiv 1 \pmod{r}$, we have $xj(n/r) \equiv n/r \pmod{n}$, so this is $a\ell(n/r) = as_{k+1}$. Also, let $s(n/n_k)$ be an arbitrary element of $S_k = \langle n/n_k\rangle$, and let $\hat{s}$ be such that $sn/n_k = (\hat{s}, 0)$ under the isomorphism discussed in the previous paragraph. Then

$$\alpha_{k+1}\beta_k(sn/n_k) = \alpha_{k+1}(sn/n_k) = \alpha_{k+1}((\hat{s}, 0)) = (x\hat{s}, 0) = x(\hat{s}, 0) = xsn/n_k.$$

Since $x \equiv 1 \pmod{n_k}$, we have $x(n/n_k) \equiv n/n_k \pmod{n}$, so $\alpha_{k+1}\beta_k$ fixes sn/n_k. We have now established the claim with which we started this paragraph, and completed the second step of our proof.

We will complete our proof by using another inductive argument to show that in fact, every vertex in S_{k+1} is fixed by β_{k+1}. Define $T_0 = S_k \cup \langle s_{k+1}\rangle$, and for $m \geq 1$,

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

It is not hard to see that every element of S_{k+1} will be in T_m for some m. We have shown above that every vertex in T_0 is fixed by β_{k+1}; this is the base case for our induction.

Notice that T_0 is a union of cosets of $\langle n/d\rangle$. We claim that every T_m is a union of cosets of $\langle n/d\rangle$. We prove this by induction before we begin our proof that every vertex of T_m is fixed by β_{k+1}, as it will be required in that proof. Suppose that $s \in T_m$. If $s \in T_{m-1}$ then by our inductive hypothesis, the coset of $\langle n/d\rangle$ that contains s is in T_{m-1}. If $s \notin T_{m-1}$ then $s - s_{k+1} \in T_{m-1}$ and there is some $1 \le y \le k$ such that $s - s_y \in T_{m-1}$. But since T_{m-1} is a union of cosets of $\langle n/d\rangle$, this means that $s - s_{k+1} + \langle n/d\rangle \subseteq T_{m-1}$ and $s - s_y + \langle n/d\rangle \subseteq T_{m-1}$, so clearly $s + \langle n/d\rangle \subseteq T_m$, as desired.

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

Notice that every coset of S_k contains some vertex of $\langle s_{k+1}\rangle$, and every coset of $\langle s_{k+1}\rangle$ contains some vertex of S_k. So since β_{k+1} fixes every vertex of T_0, we must have β_{k+1} fixes (set-wise) every coset of $\langle s_{k+1}\rangle$ and every coset of S_k. In fact, this means that β_{k+1} must fix (set-wise) every intersection of some coset of S_k with some coset of $\langle s_{k+1}\rangle$. By elementary properties of cyclic groups, these cosets all have size d, and are in fact precisely the cosets of $\langle n/d\rangle$. If $d = 1$, then these cosets are all singletons and we immediately see that every vertex of S_{k+1} is fixed by β_{k+1}; in the remainder of this proof we therefore assume that $d > 1$. Since the cosets of $\langle n/d\rangle$ are fixed set-wise, it must be the case that $\beta_{k+1}(s) = s + z(n/d)$ for some $0 \le z \le d - 1$. Towards a contradiction, let us suppose that $z \ne 0$. Let p be some prime such that p^a is a divisor of d but p^a is not a divisor of z; since $0 < z < d$ and $d > 1$, such a p exists.

Now, since β_{k+1} fixes $s - s_{k+1}$ and takes s to $s + z(n/d)$, it must take $(s - s_{k+1}) + as_{k+1}$ to $(s - s_{k+1}) + a(s_{k+1} + z(n/d))$ for any a. Notice that when $a = r/d$ we have $as_{k+1} = a\ell n/r = \ell n/d \in \langle n/d\rangle$, so since T_m is a union of cosets of $\langle n/d\rangle$, we have $(s - s_{k+1}) + as_{k+1} \in T_m$. So by our induction hypothesis β_{k+1} fixes $(s - s_{k+1}) + (r/d)s_{k+1}$. But then the first sentence of this paragraph shows that this must be the same as $(s - s_{k+1}) + (r/d)(s_{k+1} + z(n/d))$. Hence $(r/d)z(n/d) \equiv 0 \pmod{n}$. Thus, d divides $(r/d)z$. In particular, p^a divides $(r/d)z$, and since p^a does not divide z, we must have $p \mid r/d$.

Similarly, since β_{k+1} fixes $s - s_y$ and takes s to $s + z(n/d)$, it must take $(s - s_y) + as_y$ to $(s - s_y) + a(s_y + z(n/d))$ for any a. Since $S_k = \langle n/n_k\rangle$, we have $s_y = b(n/n_k)$ for some b. Notice that when $a = n_k/d$ we have $as_y = ab(n/n_k) = bn/d \in \langle n/d\rangle$, so since T_m is a union of cosets of $\langle n/d\rangle$, we have $(s - s_y) + as_y \in T_m$. So by our induction hypothesis β_{k+1} fixes $(s - s_y) + (n_k/d)s_y$. But then the first sentence of this paragraph shows that this must be the same as $(s - s_y) + (n_k/d)(s_y + z(n/d))$. Hence $(n_k/d)z(n/d) \equiv 0 \pmod{n}$. Thus, d divides $(n_k/d)z$. In particular, p^a divides $(n_k/d)z$, and since p^a does not divide z, we must have $p \mid n_k/d$. But combining this with the fact that $p > 1$ and the conclusion of the previous paragraph contradicts the definition of d. We conclude that $z = 0$, so β_{k+1} fixes s. Since s was an arbitrary vertex of T_{m+1}, this completes our induction and the proof. □

3. Acknowledgements

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

References

[1] M. Conder, T. Pisanski, and A. Žitnik, *GI*-graphs and their groups, in preparation.

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