A note on arc-transitive circulant digraphs

Cheryl E. Praeger and Jing Xu

(Communicated by R. M. Guralnick)

Abstract. We prove that, for a positive integer \( n \) and subgroup \( H \) of automorphisms of a cyclic group \( Z \) of order \( n \), there is up to isomorphism a unique connected circulant digraph based on \( Z \) admitting an arc-transitive action of \( Z \rtimes H \). We refine the Kovács–Li classification of arc-transitive circulants to determine those digraphs with automorphism group larger than \( Z \rtimes H \). As an application we construct, for each prime power \( q \), a digraph with \( q/\text{C}0 \) vertices and automorphism group equal to the semilinear group \( \Gamma\ell(1, q) \), thus proving that \( \Gamma\ell(1, q) \) is 2-closed in the sense of Wielandt.

1 Introduction

Let \( Z \) be a cyclic group of order \( n \), considered in its regular action (by multiplication) as a subgroup of the symmetric group \( \text{Sym}(Z) \). Suppose that \( Z \leq G \leq N_{\text{Sym}(Z)}(Z) \), that is to say \( G \) is a semidirect product \( Z \rtimes G_0 \), for some subgroup \( G_0 \leq \text{Aut}(Z) \) acting naturally on \( Z \). We show that, for \( n \neq 4 \), there is up to isomorphism at most one \( Z \)-circulant digraph with arc-transitive automorphism group equal to \( G \), and that for most \( n \), \( G \), such a digraph exists. A question about such digraphs arose in the course of a general investigation in \([11]\) of closures of linear groups in their natural action on vectors, and we discuss this motivating question in Section 4.

A \( Z \)-circulant is a Cayley digraph \( \Gamma = \text{Cay}(Z, S) \) with vertex set \( Z \) and arc set \( A\Gamma = \{(g, sg) \mid g \in Z, s \in S\} \), for some non-empty subset \( S \) of \( Z \setminus \{1\} \). Each \( Z \)-circulant \( \Gamma \) admits \( Z \), in its regular action, as a subgroup of automorphisms; \( \Gamma \) admits \( G \) if and only if \( S \) is \( G_0 \)-invariant; and \( G \) acts arc-transitively on \( \Gamma \) if and only if \( S \) is a \( G_0 \)-orbit in \( Z \setminus \{1\} \).

In order for \( G \) to equal \( \text{Aut}(\Gamma) \) a necessary condition is that \( \Gamma \) is connected, except for the case when \( n = 4 \) and \( G_0 = \text{Aut}(Z_4) \), where the disconnected digraph \( 2K_3 \) has this property (see Lemma 2.1). In our main theorem below we show that up to isomorphism there is a unique connected \( Z \)-circulant \( \Gamma \) on which \( G \) acts arc-transitively, and we describe the possible structures of \( \Gamma \) (and of \( G_0 \) in most cases) where \( G \) fails to equal \( \text{Aut}(\Gamma) \). Explanation of the graph-theoretic notation is given in Section 2.

Theorem 1.1. Let \( Z, n, G \) be as above. Then, up to isomorphism, there is a unique con-
nected $Z$-circulant $\Gamma$ on which $G$ acts arc-transitively. Moreover either $\text{Aut}(\Gamma) = G$ or one of the following holds:

(a) $n = p \geq 5$ is prime, $\Gamma = K_p$, and $G = \text{AGL}(1, p)$;
(b) $n = bm > 4$, where $b \geq 2$, $p$ divides $m$ for each prime $p$ dividing $b$, $\Gamma = \Sigma[\overline{R}_b]$;
(c) $n = pm$, where $p$ is prime, $5 \leq p < n$, and $\gcd(m, p) = 1$, $\Gamma = \Sigma[\overline{R}_p]$ - $p\Sigma$, $G_0 = \text{Aut}(Z_p) \times H \leq \text{Aut}(Z_p) \times \text{Aut}(Z_m)$, and $\Sigma$ is a connected $(Z_m \rtimes H)$-arc-transitive $Z_m$-circulant.

Remarks 1.2. (1) Each pair $n$, $G_0$ satisfying (a) or (c) leads to a $Z$-circulant $\Gamma$ with $\text{Aut}(\Gamma)$ larger than $G$. However in case (b) we do not specify the group $G_0$ precisely: the group $Z$ in this case has a subgroup $Y$ of order $b$, and $\Gamma = \text{Cay}(Z, S)$ where $S$ is a union of $Y$-cosets each consisting of generators for $Z$. The group $G_0$ must be transitive on $S$. In Example 1.3 we give one small example for each of cases (b) and (c).

(2) The finite arc-transitive circulants were classified independently, and via two very different methods, by István Kovács [6] and Cai Heng Li [7] in 2004. The proof of Theorem 1.1 uses this classification as its starting point. The graphs occurring in Theorem 1.1 cannot simply be read off from the classifications in [6], [7]. Indeed rather subtle arguments are needed to determine precisely the arc-transitive $Z$-circulants for which a subgroup of $Z \rtimes \text{Aut}(Z)$ (rather than the full automorphism group) acts arc-transitively. A discussion of this issue for a larger class of arc-transitive Cayley graphs is given in [8]. As mentioned above, in case (b) we have not succeeded in giving a precise description, and we would be interested to have such a description.

(3) We say that a connected arc-transitive circulant $\Gamma = \text{Cay}(Z, S)$ is generic if none of Theorem 1.1 (a), (b) or (c) holds, so that $\text{Aut}(\Gamma) = G$. In particular each generic circulant is 1-regular, that is to say, $\text{Aut}(\Gamma)$ acts regularly on the arc set of $\Gamma$. If in addition $S = S^{-1}$, so that $\Gamma$ is undirected, there exists an involution $g \in \text{Aut}(\Gamma)$ that inverts an arc $(1, s)$ (where $s \in S$) and $\text{Aut}(\Gamma) = \langle G_0, g \rangle$. In many cases the subgroup $G_0$ will be cyclic, for example, this is always so if $n$ is an odd prime power. If $\Gamma$ is generic and undirected, and $G_0$ is cyclic, then $\Gamma$ can be embedded as an orientably regular map in a closed orientable surface (see [2, Proposition 2.1]) and moreover this map is chiral since $\text{Aut}(\Gamma)$ is no larger than $Z.G_0$. This observation balances the existence result [2, Corollary 5.4] concerning regular Cayley maps for cyclic groups, showing that generic undirected circulants produce chiral maps whenever $G_0$ is cyclic. Regular maps corresponding to generic undirected circulants may constitute a convenient source of chiral maps, especially taking into account an observation made in [3, Section 1], with reference to the enumerations of regular maps of small genus in [1], that among orientably regular maps, chiral maps appear to be much rarer than the alternative reflexible maps.

Example 1.3. In these examples we write $Z$ additively as the group $\mathbb{Z}_n$ of integers modulo $n$, and $G_0$ as a subgroup of the multiplicative group $\mathbb{Z}_n^*$ so that $i^* \in G_0$ denotes the map $j \mapsto ij$. We define $\Gamma = \text{Cay}(Z, S)$ by specifying the subset $S$; and $C_m$ denotes a directed cycle of length $m$. 
(1) Example for Theorem 1.1(b). We let $n = 9$, $b = 3$, and $S = \{1, 4, 7\}$, $G_0 = \langle 4^* \rangle \cong Z_3$. This yields $\Gamma = C_3^-[\overline{K}_3]$ with $\text{Aut}(\Gamma) = S_3 \wr Z_3$.

(2) Example for Theorem 1.1(c). We let $n = 15$, $b = 5$, and $S = \{1, 4, 7, 13\}$, $G_0 = \langle 13^* \rangle \cong Z_4$. This yields $\Gamma = C_3^-[\overline{K}_5] - 5C_3^-$ with $\text{Aut}(\Gamma) = Z_3 \times S_5$.

As an application of this theorem relevant to the discussion in Section 4, we consider the connected circulant digraph $\Gamma$ for the one-dimensional semilinear group $G = \Gamma L(1, q)$, where $q = p^f$. Here $Z = \text{GL}(1, q) = \langle \zeta \rangle \cong Z_{q-1}$, where $\zeta$ is a primitive element of the field $F = GF(q)$ and we identify $Z$ with the multiplicative group of $F$. The group $G_0 = \langle \phi \rangle$ is generated by the Frobenius automorphism $\varphi : x \mapsto x^p$ of $F$. The unique connected $G$-arc-transitive $Z$-cyclic digraph $\Gamma(q)$ proved to exist in Theorem 1.1 is (up to isomorphism) $\text{Cay}(Z, S)$ with $S = \{\zeta, \zeta^p, \ldots, \zeta^{p^{f-1}}\}$. We call $\Gamma(q)$ a semilinear digraph. We prove that $\Gamma(q)$ does not arise in any of the parts (a)–(c) of Theorem 1.1 and hence obtain the following result. As a consequence we deduce that $\Gamma L(1, q)$, in its natural action on $F \setminus \{0\}$ is 2-closed in the sense of Wielandt (Corollary 4.1).

**Theorem 1.4.** The semilinear digraph $\Gamma(q)$ has automorphism group $\Gamma L(1, q)$.

Theorem 1.1 is proved in Section 3. As we mentioned in Remark 1.2, its proof uses the classification of arc-transitive circulants in [6], [7]. We review this classification, and prove some preliminary results in Section 2. The second result, Theorem 1.4, is proved in Subsection 4.1.

## 2 Arc-transitive circulant digraphs

### 2.1 Graph-theoretic notation

The notation used in the statement of Theorem 1.1 involves the following notions. We denote by $K_n$ the complete digraph on $n$ vertices in which each ordered pair of distinct vertices is an arc. The complement of $K_n$ is denoted by $\overline{K}_n$ and is the digraph with $n$ vertices and no arcs.

When we say that $\Gamma = (V, A\Gamma)$ is a digraph, we mean that $V$ is the vertex set of $\Gamma$ and $A\Gamma$ (sometimes written as $A(\Gamma)$) is its arc set. For digraphs $\Gamma = (V, A\Gamma)$ and $\Sigma = (W, A\Sigma)$, the **lexicographic product** $\Gamma[\Sigma]$ of $\Sigma$ by $\Gamma$ is the digraph $(V \times W, A(\Gamma[\Sigma]))$ such that $((v_1, w_1), (v_2, w_2))$ is an arc if and only if either $(v_1, v_2) \in A\Gamma$, or $v_1 = v_2$ and $(w_1, w_2) \in A\Sigma$.

For a positive integer $b$ and a digraph $\Gamma$, $b.\Gamma$ means the digraph consisting of $b$ vertex disjoint copies of $\Gamma$ (with no additional arcs involving vertices from distinct copies of $\Gamma$). A deleted lexicographic product, denoted by $\Gamma[\overline{K}_b] - b.\Gamma$, is a digraph whose vertex set is the vertex set of $\Gamma[\overline{K}_b]$ and whose arc set equals $A(\Gamma[\overline{K}_b]) \setminus A(b.\Gamma)$.

### 2.2 Our hypotheses, and the disconnected case

As in Section 1 let $Z$ be a finite cyclic group considered in its regular action as a subgroup of $\text{Sym}(Z)$, and let $\Gamma = \text{Cay}(Z, S)$ be a $Z$-cyclic, with $S$ a non-empty subset of $Z^\# := Z \setminus \{1\}$. Con-
sider also Aut($Z$) as a subgroup of Sym($Z$) in its natural action. Then Aut($Z$) normalizes $Z$ in Sym($Z$), and Aut($Z$) ∩ Aut($\Gamma$) is equal to

$$\text{Aut}(Z, S) := \{\sigma \in \text{Aut}(Z) \mid S^\sigma = S\}.$$ 

In fact $G := N_{\text{Aut}(\Gamma)}(Z) = Z \rtimes \text{Aut}(Z, S)$; see for example [5].

The Cayley digraph $\Gamma = \text{Cay}(Z, S)$ is said to be a normal circulant if $Z$ is normal in Aut($\Gamma$), or equivalently, if Aut($\Gamma$) = $Z \rtimes \text{Aut}(Z, S)$. We prove the assertion made in Section 1 about disconnected circulants.

**Lemma 2.1.** With the above notation, if Aut($\Gamma$) = $G$ and $\Gamma$ is not connected, then $n = 4$, $\Gamma = 2.K_2$ and Aut($\Gamma$) = $G = Z \rtimes \text{Aut}(Z) \cong D_8$.

**Proof.** Now Aut($\Gamma$) = $G = Z \rtimes \text{Aut}(Z, S)$, and the stabilizer in $G$ of the two vertices 1 and $z$, where $Z = \langle z \rangle$, is trivial. Suppose that $\Gamma = b.\Gamma_0$ with $b \geq 2$ and $n = bm$. Then $\Gamma_0$ is a $Z_m$-circulant and Aut($\Gamma$) = Aut($\Gamma_0$) ∩ $S_b$ = $Z_m$. Moreover the vertices 1 and $z$ lie in different connected components of $\Gamma$.

If $b \geq 3$, then the stabilizer in Aut($\Gamma_0$) ∩ $S_b$ of two vertices in different components contains a copy of Aut($\Gamma_0$) acting on a third component, which is not possible. Hence $b = 2$ and Aut($\Gamma_0$) ∩ $S_2$ contains an element $g$ of order $m$ that fixes pointwise the connected component $\Gamma'$ containing 1$_Z$ (which has vertex set $\langle z^2 \rangle$), and induces an $m$-cycle on the other component. Now $g \in$ Aut($Z, S$) since $g$ fixes 1$_Z$, and as $g$ fixes the vertex $z^2$ of $\Gamma'$ it follows that $z^g = z^i \neq z$, for some $i$, and $z^2 = (z^2)^2 \neq z^{2i}$. Thus $i \equiv m + 1 \pmod{n}$ and since $o(z) = o(z^g)$, $m$ must be even. Then $z^{g^2} = z^{(m+1)^2} = z$, and since $g$ acts as an $m$-cycle on the component containing $z$, we must have $m = 2$. This means that $S = \{z^2\}$, $\Gamma = 2.K_2$ and Aut($\Gamma$) = $G = Z \rtimes \text{Aut}(Z) \cong D_8$. □

### 2.3 The classification.

The classification theorem, proved in [6, Theorem 1] and [7, Theorem 1.3], shows that most connected arc-transitive circulants are normal.

**Theorem 2.2 ([6], [7]).** Let $Z$ be a cyclic group of order $n$ and let $\Gamma$ be a connected arc-transitive $Z$-circulant. Then one of the following holds where, in (b) and (c), $\Sigma$ is a connected arc-transitive $Z_m$-circulant:

(a) $\Gamma = K_n$;
(b) $\Gamma = \Sigma[K_b]$, where $n = bm$, $2 \leq b < n$;
(c) $\Gamma = \Sigma[K_b] - b.\Sigma$, where $n = bm$, $4 \leq b < n$, gcd($b, m$) = 1;
(d) $\Gamma$ is a normal circulant.

### 2.4 Making the cases of Theorem 2.2 disjoint.

We make some remarks about the automorphism groups of the $Z$-circulants $\Gamma = \text{Cay}(Z, S)$ occurring in cases (a)–(c) of Theorem 2.2. In case (a) of Theorem 2.2, $S = Z \setminus \{1\}$ and Aut($\Gamma$) = $S_n$ so $Z$ is normal in Aut($\Gamma$) if and only if $n \leq 3$; and none of the digraphs of part (b) or (c) is complete.
Discussion of cases (b) and (c) involves the notion of a quotient digraph defined as follows. For \( Z \leq G \leq \text{Sym}(Z) \), a partition \( \mathscr{B} = \{ B_1, \ldots, B_m \} \) of \( Z \) is called a block system for \( G \) if each element \( g \in G \) permutes the parts of \( \mathscr{B} \) (that is \( B_i^g \in \mathscr{B} \) for each \( i \)). It is not difficult to show that each block system for \( G \) must be the set of cosets of some subgroup of \( Z \) (this is essentially \cite[Theorem 3(a)]{8}, but the converse is not true in general. In particular, all blocks of a block system for \( G \) have the same size. The block system is called trivial if \( |B_i| = 1 \) or \( |\mathscr{B}| = 1 \), and otherwise is said to be non-trivial; \( \mathscr{B} \) is called minimal and its elements are called minimal blocks if \( \mathscr{B} \) is non-trivial and the only block system that properly refines it is the trivial one with blocks of size 1.

If \( Z \leq G \leq \text{Aut}(\Gamma) \) for some \( Z \)-circulant \( \Gamma \), then each block system \( \mathscr{B} \) for \( G \) gives rise to a quotient digraph \( \Gamma_{\mathscr{B}} \), defined as the digraph with vertex set \( \mathscr{B} \) such that \((B_i, B_j)\) is an arc if and only if \((u, v) \in A\Gamma \) for some \( u \in B_i \) and \( v \in B_j \). Now \( \mathscr{B} \) is the set of \( Y \)-cosets in \( Z \), for some \( Y < Z \), and the quotient digraph \( \Gamma_{\mathscr{B}} \) admits an induced action of \( G \) in which the subgroup \( Z \) induces the regular cyclic group \( Z/Y \). Thus \( \Gamma_{\mathscr{B}} \) is a \((Z/Y)\)-circulant, and it is connected if \( \Gamma \) is connected.

In case (b) of Theorem 2.2, since \( n = mb \) the group \( Z \) has a (unique) subgroup \( Y \cong Z_b \), and \( Z < G \leq \text{Aut}(\Gamma) \) where \( G = S_b \triangleleft \text{Aut}(\Sigma) \). The set \( \mathscr{B} \) of \( Y \)-cosets in \( Z \) is a block system for \( G \) and \( \Gamma_{\mathscr{B}} \cong \Sigma \) is a connected \((Z/Y)\)-circulant. Note that the integer \( b \) and quotient graph \( \Sigma \) may not be uniquely determined. For example, the integers \( Z \cong [K]\) and if this is the case then \( \Gamma \cong \Sigma'[K_{bb}] \) with \( \Sigma' \) a \((Z/Y')\)-circulant, where \( |Y'| = bb' \).

**Lemma 2.3.** Let \( \Gamma, n, Z, b, m \) be as in Theorem 2.2(b). Then

1. \( \Gamma \) is normal if and only if \( b = m = 2 \), and in this case \( \Gamma \cong C_4 \).
2. If \( b \) maximal such that \( \Gamma \cong \Sigma[K] \) and \( G, Y, \mathscr{B} \) are as above, then the set of \( Y \)-cosets in \( Z \) is the unique minimal block system for \( \text{Aut}(\Gamma) \), and \( \text{Aut}(\Gamma) = S_b \triangleleft \text{Aut}(\Sigma) \).

**Proof.** Suppose first that \( \Gamma \) is normal, that is, \( Z < S_b \triangleleft \text{Aut}(\Sigma) \). Now \( Z \cap S_b^{m} \) is a diagonal subgroup isomorphic to \( Z_b \) and normal in \( S_b^{m} \), and hence \( b = 2. \) Let \( Z = \langle z \rangle \). Then we may assume that \( z = ax \) where

\[
\sigma = (12 \ldots m) \in S_m \quad \text{and} \quad x = (x_1, \ldots, x_m) \in S_2^m.
\]

This implies that we have \( \sigma^m = (t, t, \ldots, t) \) where \( t = x_1 x_2 \ldots x_m \in S_2 \setminus \{1\} \). For \( u = (t, 1, \ldots, 1) \), the conjugate \( \sigma^u = uzu = z(t, t, 1, \ldots, 1) \in Z \), and since the only elements of \( Z \) that project to \( \sigma \) modulo \( S_2^m \) are \( z \) and \( z(t, t, \ldots, t) \), it follows that \( m = 2 \). Conversely if \( b = m = 2 \), then \( \Gamma = C_4 \) and \( Z < \text{Aut}(\Gamma) = S_2 \triangleleft S_2 = D_8 \), so \( \Gamma \) is normal. (This could also be deduced from \cite[Theorem 6.1]{4}, see also \cite[Theorem 3]{6}, but information about the group is not so easy to extract.)

Now let \( b \) be maximal as in (2). Let \( \mathscr{B}_0 \) be the set of \( Y \)-cosets in \( Z \) and let \( x \in B_0 \in \mathscr{B}_0 \). Then \( G_{\mathscr{B}_0}^B = S_b \) is primitive, so the only \( G \)-invariant partition of \( Z \) refining \( \mathscr{B}_0 \) is the trivial block system for \( G \) with blocks of size 1. Thus \( \mathscr{B}_0 \) is a minimal block system for \( G \).
Since $\Gamma$ is not a complete graph, $\text{Aut}(\Gamma) \neq S_n$. Hence, since $G$ contains a transposition, it follows that $\text{Aut}(\Gamma)$ has at least one non-trivial block system on $Z$, say $\mathcal{B}$ (see [9, Theorem 13.2]). Let $x \in B \in \mathcal{B}$. If $B \cap B_0 = \{x\}$, then for $x' \in B_0 \setminus \{x\}$, $G$ contains the transposition $g = (x, x')$ and $B^g \cap B = B \setminus \{x\}$ which is a contradiction. Thus $|B \cap B_0| \geq 2$, and hence $B \cap B_0$ is a non-trivial block generating a non-trivial block system for $G$ refining $\mathcal{B}_0$. By the minimality of $\mathcal{B}_0$, it follows that $B$ contains $B_0$. This implies moreover that $B$ is a union of blocks from $\mathcal{B}_0$, that $G_B$ contains $G_{B_0}$, and hence that the group $G_B^B$ induced on $B$ contains a transposition.

Suppose now that $\mathcal{B}$ is a minimal block system for $\text{Aut}(\Gamma)$. Then the stabilizer $\text{Aut}(\Gamma)_B$ induces a primitive group on $B$, and we have just seen that this primitive group contains a transposition. Thus $\text{Aut}(\Gamma)_B^B = \text{Sym}(B)$. Let $K$ be the kernel of the action of $\text{Aut}(\Gamma)$ on $\mathcal{B}$. Then $K \neq 1$ since it contains the kernel $S_m^B$ of the action of $G$ on $\mathcal{B}_0$. Hence $K^B$, a normal subgroup of $\text{Aut}(\Gamma)_B^B$ containing $(S_m^B)^B$, is equal to $\text{Sym}(B)$. Moreover, since the pointwise stabilizer in $G$ of $Z \setminus B_0$ is $S_b$, it follows that $K = \prod_{B^B \in \mathcal{B}} \text{Sym}(B^B)$.

Note in particular that $B$ contains no edges of $\Gamma$. Let $\{x, \beta\}$ be an edge of $\Gamma$ and let $B' \in \mathcal{B}$ be the block containing $\beta$. Then since $K$ contains $\text{Sym}(B) \times \text{Sym}(B')$ it follows that each vertex of $B$ is joined by an edge to each vertex of $B'$. Thus $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_{b'}]$ where $b' = |B|$. By hypothesis, $b$ is maximal such that $\Gamma$ can be expressed in this way, and hence $b' = b$, $\mathcal{B} = \mathcal{B}$, and $\text{Aut}(\Gamma) = S_b \wr \text{Aut}(\Sigma)$. This proves (2).

**Remark 2.4.** In case (c) of Theorem 2.2, since $\gcd(b, m) = 1$, the group $Z$ is a direct product $M \times Y$ with $M \cong Z_m$ and $Y \cong Z_b$. Moreover, $\Gamma = \text{Cay}(Z, S)$ where $S = Y^* \times T$ and $T \subseteq M^*$. This follows from Remark 2.4. Suppose also that $\Gamma = \Gamma[\overline{K}_{b'}]$ as in Theorem 2.2(b). Then $b'$ divides $m$, and for $Z_{b'} \cong Y' < M < Z$, $T$ is a union of cosets of $Y'$ in $M \setminus Y'$. Also, setting $\Sigma' := \Gamma_{\mathcal{B}'} = \text{Cay}(M / Y', T / Y')$ where $\mathcal{B}'$ is the set of $Y'$-cosets in $M$,$$
abla' \cong \Sigma'[\overline{K}_{b'}] - b\Sigma', \quad \text{and} \quad \Sigma \cong \Sigma'[\overline{K}_{b'}].$$

**Lemma 2.5.** Let $\Gamma, n, Z, b, m, \Sigma$ be as in Theorem 2.2(c) and let $Z = Y \times M$, $G, S, T, \mathcal{B}$ be as in Remark 2.4. Suppose also that $\Gamma = \Gamma[\overline{K}_{b'}]$ as in Theorem 2.2(b). Then $b'$ divides $m$, and for $Z_{b'} \cong Y' < M < Z$, $T$ is a union of cosets of $Y'$ in $M \setminus Y'$. Also, setting $\Sigma' := \Gamma_{\mathcal{B}'} = \text{Cay}(M / Y', T / Y')$ where $\mathcal{B}'$ is the set of $Y'$-cosets in $M$,$$
abla' \cong \Sigma'[\overline{K}_{b'}] - b\Sigma', \quad \text{and} \quad \Sigma \cong \Sigma'[\overline{K}_{b'}].$$

**Proof.** In this case $\Gamma = \text{Cay}(Z, S)$ with $S = Y^* \times T$ for some $T \subseteq M^*$. Set $x := 1_Z$. Fix $\beta \in \mathcal{B}$ such that $(x, \beta)$ is an arc; then $\beta = yt$ with $y \in Y^*$ and $t \in T$. Suppose that Theorem 2.2(b) also holds for $\Gamma$, say $\Gamma \cong \Gamma[\overline{K}_{b'}]$. Let $B_0$ be the set of $Y'$-cosets in $Z$, where $Y' < Z$ of order $b'$, so that $B_0 = Y'$ is the block of $\mathcal{B}_0$ containing $x$. Now $B_0$ contains no arcs, and so $\beta \notin B_0$. Suppose that $B_0$ contains a vertex $\gamma = y'x$, where $y' \in Y^*$, $x \in M$. By the definition of $\Gamma = \text{Cay}(Z, S)$, it follows that $(x, y')$ is also an arc, and since $\Gamma = \Gamma[\overline{K}_{b'}]$ it follows further that $\text{Aut}(\Gamma)$ contains the transposition
Throughout this section let \( g = (x, y) \). This implies that \( (y'x, y't) = (x, y't)^g \) is an arc, contradicting the fact that \( \Gamma = \text{Cay}(Z, S) \). Thus \( B_0 \subseteq M \) and so \( b' \) divides \( m \), \( Y' \leq M \), and as \( B_0 \) contains no arcs, \( T \subseteq M \setminus Y' \).

The image \( B_0yt \) of \( B_0 \) under multiplication by \( yt \) is the block of \( \mathcal{B}_0 \) containing \( \beta = yt \). Since \( \Gamma = \Gamma'[\mathcal{K}_{b'}] \) and \( (x, \beta) \) is an arc, it follows that \( (x, h) \) is an arc for each \( h \in B_0yt \), and hence that \( T \) contains \( B_0t = Y't \). Thus \( T \) is a union of \( Y' \)-cosets. It now follows that \( \Sigma \cong \Sigma'[\mathcal{K}_{b'}] \) and \( \Gamma' \cong \Sigma'[\mathcal{K}_b] - b\Sigma' \), where \( \Sigma' := \Gamma_\mathcal{B}' = \text{Cay}(M/Y', T/Y') \), with \( \mathcal{B}' \) the set of \( Y' \)-cosets in \( M \). \( \square \)

The discussion above shows how the various cases of Theorem 2.2 may overlap. We use the following disjoint case division in our proof in the next section.

**Lemma 2.6.** Let \( Z, n, \Gamma \) be as in Theorem 2.2. Then exactly one of the following holds where, in (b') and (c'), \( \Sigma \) is a connected arc-transitive \( Z_m \)-circulant:

(a') \( \Gamma = K_n \) with \( n \geq 4 \);

(b') \( \Gamma = \Sigma[\mathcal{K}_b] \), where \( n = bm > 4 \) and \( 2 \leq b < n \);

(c') \( \Gamma = \Sigma[\mathcal{K}_b] - b.\Sigma \), where \( n = bm, 4 \leq b < n, \, \gcd(b, m) = 1 \), and \( \Sigma \) is not \( \Sigma'[\mathcal{K}_{b'}] \) for any \( b' > 1 \) dividing \( m \);

(d') \( \Gamma \) is a normal circulant.

**Proof.** If Theorem 2.2(a) holds then by the first paragraph of this subsection, either (d) holds with \( n \leq 3 \), or (a') holds with \( n \geq 4 \). If Theorem 2.2(b) holds, then by Lemma 2.3, either (d) holds with \( n = 4 \), or (b') holds with \( n > 4 \).

Finally suppose that Theorem 2.2(c) holds, and let \( G, Z = M \times Y \), and \( \mathcal{B} \) be as in Remark 2.4, with \( \Gamma = \Sigma[\mathcal{K}_b] - b.\Sigma \). Let \( z = 1 \in Y \) with \( Y \) considered as a block of \( \mathcal{B} \). Since \( b \geq 4 \), \( Z \cap S_b = Y \) is not normal in \( S_b \) and hence \( \Gamma \) is not normal. Also \( \Gamma \) is not a complete graph. If also Theorem 2.2(b) holds for \( \Gamma \), say \( \Gamma = \Gamma'[\mathcal{K}_{b'}] \) for some \( b' > 1 \), then it follows from Lemma 2.5 that \( b' \) divides \( m \) and \( \Sigma \cong \Sigma'[\mathcal{K}_{b'}] \). Thus exactly one of (b') and (c') holds. \( \square \)

### 3 Proof of Theorem 1.1

Throughout this section let \( Z, \Gamma = \text{Cay}(Z, S), G \) be as in Subsection 2.2, and assume that \( \Gamma \) is connected and \( G \) acts arc-transitively on it. Write \( G_0 := \text{Aut}(Z, S) \). First we prove the uniqueness of \( \Gamma \) up to isomorphism.

**Lemma 3.1.** There is, up to isomorphism, a unique connected \( Z \)-circulant \( \Gamma \) on which \( G \) acts arc-transitively. Moreover, if \( \Gamma \) is a normal circulant then \( \text{Aut}(\Gamma) = G \).

**Proof.** Since \( \Gamma = \text{Cay}(Z, S) \) is connected, \( S \) is a generating set of \( Z \), and since \( G \) acts arc-transitively, its subgroup \( G_0 \) is transitive on \( S \). This implies that each element of \( S \) is a generator of \( Z \) and \( S = z^G_0 \) for some generator \( z \). Let \( \Gamma' = \text{Cay}(Z, S') \) be another connected \( Z \)-circulant admitting an arc-transitive action of \( G \). Then we
also have $S' = (z')^{G_0}$ with $z'$ a generator for $Z$. Now $\text{Aut}(Z)$ is transitive on the set of generators for $Z$, and so there exists $\sigma \in \text{Aut}(Z)$ such that $z^\sigma = z'$. Moreover $\text{Aut}(Z)$ is abelian so $\sigma$ normalizes $G_0$ and we have $S^\sigma = (z^{G_0})^\sigma = (z^\sigma)^{G_0} = S'$. This implies that $\sigma$, considered as an element of $\text{Sym}(Z)$, is a graph isomorphism from $\Gamma$ to $\Gamma'$. Thus the uniqueness assertion is proved. Finally if $\Gamma$ is normal, then $\text{Aut}(\Gamma) = \text{Aut}(\Gamma) \cap \text{N}_{\text{Sym}(Z)}(Z) = G$. 

To complete the proof of Theorem 1.1 we assume that $\Gamma$ is not a normal $Z$-circulant and consider cases (a'), (b'), (c') of Lemma 2.6 in turn.

**Lemma 3.2.** If Lemma 2.6(a') holds then Theorem 1.1(a) holds.

**Proof.** Suppose that $\Gamma = K_n$ with $n \geq 4$. Then $G_0$ is transitive on $S = Z \setminus \{1_Z\}$, and hence $n = p$ is prime, so $p \geq 5$ and $G = \text{AGL}(1, p)$. 

**Lemma 3.3.** If Lemma 2.6(b') holds then Theorem 1.1(b) holds.

**Proof.** Suppose that $\Gamma = \Sigma[\overline{K}_b]$, where $n = bm > 4$ and $2 \leq b < n$. Let $Y \leq Z$ with $Y \cong Z_b$. Then $S$ is a union of cosets of $Y$ and $G_0 = \text{Aut}(Z, S)$ is transitive on $S$. Let $z \in S$ so that $Yz \subseteq S$. Then $p$ be a prime dividing $b$ and let $P$ be the Sylow $p$-subgroup of $Z$. Then $z = z_1z_2$ where $z_1 \in P$ and $z_2$ has order coprime to $p$. If $P \subseteq Y$, then $z_2 = z_1^{-1}z \in Yz \subseteq S$, contradicting the condition that every element of $S$ must be a generator for $Z$. Thus $P \not\subseteq Y$ and so $p$ must divide $m$. 

**Lemma 3.4.** If Lemma 2.6(c') holds then Theorem 1.1(c) holds.

**Proof.** Suppose that $\Gamma = \Sigma[\overline{K}_b] - b, \Sigma$, where $n = bm$, $4 \leq b < n$, and $\gcd(b, m) = 1$. Then $Z = M \times Y$ with $M \cong Z_m$ and $Y \cong Z_b$, and $S$ is a union of subsets of the form $x(Y \setminus \{1_Y\})$, where $x \in M$. Let $z \in S$ so that $z = z_1z_2$ where $z_1$, $z_2$ is a generator of $M$, $Y$ respectively. Then $S$ contains $z_1(Y \setminus \{1_Y\})$, and it follows that $o(z_1z_2) = o(z_1y)$ for each $y \in Y \setminus \{1_Y\}$. Since $\gcd(b, m) = 1$ it follows that $o(z_2) = o(y)$ for each $y \in Y \setminus \{1_Y\}$, and hence $b$ is prime. Finally, since $G_0$ is transitive on $S$ we must have $G_0 = \text{Aut}(Y) \times H$ for some $H \leq \text{Aut}(M)$. 

The proof of Theorem 1.1 now follows from Lemmas 3.1, 3.2, 3.3 and 3.4.

### 4 Closures and circulants

The motivation for this investigation was a study in [11] of closures of linear groups in the sense of Wielandt [10]. The linear groups considered were subgroups of the group $\Gamma L(d, q)$ of semi-linear transformations acting on the vector space $V = V(d, q)$ of $d$-dimensional row vectors over the field $F = GF(q)$ of order $q$. For $G \leq \Gamma L(d, q)$ and $k \geq 1$, each $G$-invariant subset of the Cartesian product $V^k$ (under the natural induced $G$-action) is called a $k$-relation for $G$, and the largest permutation
group on $V$ preserving each $k$-relation of $G$ is called the $k$-closure of $G$ on $V$, and denoted by $G^{(k)}$. The question addressed in [11] was the extent to which membership of an element $g \in \Gamma L(d, q)$ in $G^{(k)}$ could be determined by testing $g$-invariance of a small number of geometrically based $k$-relations, possibly just one.

This turns out to be the case for many types of groups $G$. For example, if $G$ preserves on $V$ the structure of an $c$-dimensional vector space $V(c, q^b)$ over an extension field $K$ of $F$ of order $q^b$, where $d = bc$ and $b > 1$, then $G$ leaves invariant the 2-relation $\Delta$ consisting of all pairs $(u, v)$ such that $u, v$ generate the same 1-dimensional $K$-subspace of $V$. For the case when $c$ is also at least 2, so that $\Delta \neq V^2$, it was shown in [11, Proposition 4.3.2] that $g \in \Gamma L(d, q)$ lies in $G^{(2)}$ if and only if $g$ leaves invariant the single 2-relation $\Delta$. This raised the question as to whether there might also be a single 2-relation $\Delta$ in the case $c = 1$ such that checking invariance of $\Delta$ would be sufficient to prove membership of $G^{(2)}$.

In the case where $c = 1$ and $d \geq 2$, the largest group preserving the structure $V = V(1, q^d)$ is the semilinear subgroup $G = \Gamma L(1, q^d) < \Gamma L(d, q)$. Now $G$ acting on $V^* := V \setminus \{0\}$ contains the cyclic regular subgroup $Z := \text{GL}(1, q^d)$, and each 2-relation for $G$ contained in $(V^*)^2$ may be viewed as the arc set of a $Z$-circulant digraph $\Gamma$ with vertex set $V^*$ admitting $G$ as a vertex-transitive group of automorphisms. For the minimal such 2-relations, $G$ acts arc-transitively. Thus our question becomes: if we test that $g \in \Gamma L(d, q)$ is an automorphism of such a minimal $Z$-circulant digraph $\Gamma$, can we conclude that $g$ lies in $G$? In other words: does $\text{Aut}(\Gamma) \cap \Gamma L(d, q) = G$ for some $\Gamma$?

By Theorem 1.4, the semilinear graph $\Gamma(q^d)$ has automorphism group equal to $G$. Thus the arc set of $\Gamma(q^d)$, namely $\Delta = \{(x, x\xi^i) \mid 0 \leq i < df\}$ where $\xi$ is a primitive element of $K = \text{GF}(q^d)$, has the (even stronger) property that if $g \in \text{Sym}(V^*)$ leaves $\Delta$ invariant then $g \in G$. This yields the following corollary to Theorem 1.4 (where we write $q$ for the quantity $q^d$ in the above discussion).

**Corollary 4.1.** Let $G = \Gamma L(1, q) \subseteq \text{Sym}(V^*)$, where $V = V(1, q)$ and $q = p^f$ with $p$ prime and $f \geq 1$. Then $g \in G^{(2)}$ if and only if $g$ leaves invariant the arc set $\{(x, x\xi^i) \mid x \in \text{GF}(q), \ 0 \leq i < f\}$ of $\Gamma(q)$, where $\xi$ is a primitive element of $\text{GF}(q)$. In particular $G = G^{(2)}$.

What remains is for us to prove Theorem 1.4.

**4.1 Proof of Theorem 1.4.** Let $q = p^f$ where $p$ is a prime and $f \geq 1$, and let $Z = \langle \xi \rangle$, the multiplicative group of a field of order $q$. Consider the semilinear digraph $\Gamma = \Gamma(q) = \text{Cay}(Z, S)$, where $S = \{\xi, \xi^2, \ldots, \xi^{p^f-1}\}$. Then $\Gamma$ is a connected $Z$-circulant admitting an arc-transitive action of $G = \Gamma L(1, q) = Z \rtimes G_0$ where $G_0 = \langle \varphi \rangle$ is generated by the Frobenius automorphism $\varphi : x \mapsto x^p$.

If $f = 1$ then $\Gamma$ is a directed cycle with automorphism group equal to $Z$ which equals $G$ in this case. We therefore assume that $f \geq 2$, and we prove that $\Gamma(q)$ does not arise in any of the parts (a)–(c) of Theorem 1.1. If $\Gamma$ is a complete graph then $S = Z \setminus \{1_Z\}$ so $q - 1 = f$, implying that $q = p^f = 2$, which contradicts $f \geq 2$. Thus Theorem 1.1(a) does not hold.
The prime arguments use the concept of a primitive prime divisor of $p^f - 1$. This is a prime divisor $r$ of $p^f - 1$ such that $r$ does not divide $p^i - 1$ for any $i < f$. It was shown by Zsigmondy [12] that such a prime exists unless either $(p, f) = (2, 6)$, or $f = 2$ and $p + 1$ is a power of 2. Moreover, for each primitive prime divisor $r$ of $p^f - 1$, $p$ has order $f$ modulo $r$ and consequently $f$ divides $r - 1$, so that $r \geq f + 1$.

Suppose next that Theorem 1.1(b) holds. Then $p^f - 1 = bm > 4$ where $b \geq 2$ and $r$ divides $m$ for each prime $r$ dividing $b$. Also $S$ is a union of cosets of the subgroup $Y$ of $Z$ of order $b$. Let $y := \xi^{(p^f-1)/b}$ so that $Y = \langle y \rangle$. Then the coset $\xi Y$ is contained in $S$ and in particular $\xi y \in S$. This implies that $\xi y = \xi^{b^i}$ for some $i$ with $1 \leq i \leq f - 1$. Thus $y = \xi^{p^i - 1}$ and hence $p^f - 1 = b(p^i - 1)$. The divisibility condition on $m = p^f - 1$ is that, for each prime $r$ dividing $b$, $r$ divides $p^i - 1$. This implies that $p^f - 1$ has no primitive prime divisor. If $(p, f) = (2, 6)$, there are no factorizations $63 = b(2^i - 1)$ with the required divisibility property. Thus $f = 2$ and $b = p + 1 = 2^a > 4$. Therefore $|S| = f = 2$ and $S$ is a union of $Y$-cosets, so that $b = |Y| = 2$ which is a contradiction.

Finally suppose that Theorem 1.1(c) holds. Then $n = bm$, $5 \leq b < n$, $b$ is prime, and $\gcd(b, m) = 1$ so that $ab + cm = 1$ for some integers $a, c$. Set $x := \xi^b$, $y := \xi^m$ and $Y := \langle y \rangle$ so that $Z \cong \langle x \rangle \times Y$ and $S$ is a union of subsets of the form $x^i(Y \setminus \{1_Y\})$, for some $i$. In particular $f = |S| > b - 1 \geq 4$, and $\xi = x^{a} y^{c'}$ where $0 \leq c' < b$ and $c' \equiv c \pmod{b}$. Moreover $c' \neq 0$ since $\xi$ is a generator, and since $\xi \in S$, for each of the $b - 1$ integers $d$ satisfying $0 \leq d \leq b - 1$ and $d \neq b - c'$, the product $\xi y^d \in S$ and hence $\xi y^d = \xi^{b^i d}$ for some $i(d)$ such that $0 \leq i(d) \leq f - 1$. This is equivalent to $md = p^{i(d)} - 1$. Thus distinct integers $d$ correspond to distinct integers $i(d)$. If $b - 1 = f$, then the $f$ distinct integers $i(d)$ take on each of the $f$ integers $0, 1, \ldots, f - 1$ exactly once. In particular, there exists $d$ such that $i(d) = 1$.

We claim that this is the case, that is, that $b = f + 1$. If $p^f - 1 = bm$ has no primitive prime divisor then, since $f \geq 4$, we must have $p = 2$, $f = 6$. Then since $b$ is a prime at least 5, it follows that $b = 7 = f + 1$. On the other hand suppose that $p^f - 1$ has a primitive prime divisor $r$. Since, for all $d$, $md = p^{i(d)} - 1$ with $i(d) < f$, the prime $r$ does not divide $m$, and hence $r = b$. This implies that $b \geq f + 1$ and since we also have $b \leq f + 1$ equality holds. This proves the claim.

Thus we do have an integer $d$ such that $i(d) = 1$. For this $d$ we have $md = p - 1$, so $d \neq 0$ and $m \leq p - 1$. Thus $p^f - 1 = (f + 1)m \leq (f + 1)(p - 1)$, which holds only if $p = f = 2$, and this contradicts the fact that $f \geq 4$. This completes the proof of Theorem 1.4.

References


Received 5 November, 2007; revised 22 January, 2008

Cheryl E. Praeger, School of Mathematics and Statistics, The University of Western Australia, Crawley WA 6009, Australia

Jing Xu, LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, China
E-mail: xujing@math.pku.edu.cn