CLASSIFYING ARC-TRANSITIVE CIRCULANTS OF SQUARE-FREE ORDER

Caiheng Li[1]
Department of Mathematics and Statistics
University of Western Australia
Nedlands, WA 6907
Australia

Dragan Marušič[2]
IMFM, Oddelek za matematiko
Univerza v Ljubljani
Jadranska 19, 1000 Ljubljana
Slovenija

Joy Morris
Department of Mathematics and Statistics
Simon Fraser University
Burnaby, B. C.
Canada, V5A 1S6

Abstract

A *circulant* is a Cayley graph of a cyclic group. Arc-transitive circulants of square-free order are classified. It is shown that an arc-transitive circulant Γ of square-free order n is one of the following: the lexicographic product $\Sigma[\overline{K}_b]$, or the deleted lexicographic $\Sigma[\overline{K}_b] - b\Sigma$, where $n = bm$ and Σ is an arc-transitive circulant, or Γ is a *normal* circulant, that is, $\mathrm{Aut}\Gamma$ has a normal regular cyclic subgroup.

Keywords: circulant graph, arc-transitive graph, square-free order, cyclic group, primitive group, imprimitive group.

[1]Li is grateful to the Institute of Mathematics, Physics and Mechanics at the University of Ljubjana for hospitality and finacial support during his visit that led to the completion of this work.

[2]Supported in part by the "Ministrstvo za znanost in tehnologijo Republike Slovenije", project no. J1-101-04965-99.

1 Introductory remarks

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.

Let Γ be a graph and G a subgroup of its automorphism group $\mathrm{Aut}\,\Gamma$. The graph Γ is said to be *G-arc-transitive* if G acts transitively on the set of arcs of Γ. In particular, Γ is said to be *arc-transitive* if Γ is $\mathrm{Aut}\Gamma$-arc-transitive. Note that an arc-transitive graph Ga is necessarily vertex-transitive, that is, its automorphism group acts transitively on the vertex set $V\Gamma$ of Γ.

Given a group G and a symmetric subset $S = S^{-1}$ of $G \setminus \{id\}$, the *Cayley graph of G relative to S*, denoted by $\mathrm{Cay}(G, S)$, has vertex set G and edges of the form $\{g, gs\}$, for all $g \in G$ and $s \in S$. By the definition, the group G acting by right multiplication is a subgroup of $\mathrm{Aut}\,\Gamma$ and acts regularly on $V\Gamma = G$. The converse also holds (see [6]). A *circulant* is a Cayley graph of a cyclic group. Thus a graph Γ is a circulant of order n if and only if $\mathrm{Aut}\,\Gamma$ contains a cyclic subgroup of order n which is regular on $V\Gamma$.

A classification of 2-arc-transitive circulants was given in [1]. It was proved that a connected, 2-arc-transitive circulant of order n, $n \geq 3$, is one of the following graphs: the cycle C_n, the complete graph K_n, the complete bipartite graph $K_{\frac{n}{2},\frac{n}{2}}$, $n \geq 6$, or $K_{\frac{n}{2},\frac{n}{2}} - \frac{n}{2}K_2$ where $\frac{n}{2} \geq 5$ odd (the complete bipartite graph $K_{\frac{n}{2},\frac{n}{2}}$ minus a 1-factor).

In this paper we take the next step in our pursuit of a classification of all arc-transitive circulants, by classifying all such graphs of square-free order. To describe this classification, a few words on the notation are in order. For two graphs Γ and Σ, denote by $\Sigma[\Gamma]$ the *lexicographic product* of Γ by Σ. If in addition, Γ and Σ have the same vertex set then denote by $\Sigma - \Gamma$ the graph with vertex $V\Gamma$ and having two vertices adjacent if and only if they are adjacent in Σ but not adjacent in Γ. Furthermore, let $\overline{\Sigma}$ denote the complement of Σ, and for a positive integer m, denote by $m\Sigma$ the graph which consists of m disjoint copies of Σ. A circulant Γ is called a *normal circulant* if $\mathrm{Aut}\,\Gamma$ contains a cyclic regular normal subgroup. The following is the main result of this paper.

Theorem 1.1 *Let Γ be an arc-transitive circulant graph of square-free order n. Then one of the following holds:*

(1) Γ *is a complete graph;*

(2) Γ *is a normal circulant graph;*

(3) $\Gamma = \Sigma[\overline{K}_b]$ *or* $\Gamma = \Sigma[\overline{K}_b] - b\Sigma$*, where* $n = mb$*, and* Σ *is an arc-transitive circulant of order* m*.*

Remark 1.2 Let Γ be a connected arc-transitive circulant. If $\Gamma = \Sigma[\overline{K}_b]$ or if $\Gamma = \Sigma[\overline{K}_b] - b\Sigma$, then the graph Γ may be easily reconstructed from a smaller arc-transitive circulant Σ. Thus the graphs in part (3) of Theorem 1.1 are well-characterized. As for arc-transitive normal circulants, the following observations are in order. For two groups G and H, denote by $G \rtimes H$ a semidirect product of G by H. Assume that $\Gamma = \mathrm{Cay}(R, S)$ is normal. Let $\mathrm{Aut}(R, S) = \{\sigma \in \mathrm{Aut}(R) \mid S^\sigma = S\}$. Then by [4, Lemma 2.1], $\mathrm{Aut}\,\Gamma = R \rtimes \mathrm{Aut}(R, S)$, and since Γ is arc-transitive, $\mathrm{Aut}(R, S)$ is transitive on S. Thus S may be written as $\{s^\sigma \mid \sigma \in \mathrm{Aut}(R, S)\}$ where $s \in S$, that is, S is an $\mathrm{Aut}(R, S)$-orbit under the $\mathrm{Aut}(R)$-action. As R is cyclic, $\langle s \rangle = R$ if and only if $\langle S \rangle = R$. Hence, since Γ is connected, s generates R. This provides us with a general method for constructing connected arc-transitive normal circulants, that is, for any generating element g of R and a subgroup H of $\mathrm{Aut}(R)$, $\mathrm{Cay}(R, g^H)$ is a connected arc-transitive normal circulant. Note that, since R is cyclic, $\mathrm{Aut}(R)$ is abelian.

2 Proof of Theorem 1.1

This section is devoted to proving Theorem 1.1. We use a standard notation and terminology, see for example [3]. Let Γ be a finite graph, and assume that $G \leq \mathrm{Aut}\,\Gamma$ is transitive on $V\Gamma$. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ be a G-invariant partition of $V\Gamma$, that is, for each B_i and each $g \in G$, either $B_i^g \cap B_i = \emptyset$, or $B_i^g = B_i$. A partition $\mathcal{B}'$ is called a *refined* partition of a partition $\mathcal{B}$ if a block of $\mathcal{B}'$ is a proper subset of a block of $\mathcal{B}$. For $B \in \mathcal{B}$, denote by G_B the subgroup of G which fixes B setwise, and by G_B^B the permutation group induced by G_B on B. The *kernel* N of G on $\mathcal{B}$ is the subgroup of G in which every element fixes all $B \in \mathcal{B}$. Clearly, N is a normal subgroup of G. A partition $\mathcal{B}$ is said to be *minimal* if $\mathcal{B}$ has no refined partitions. It follows that if $\mathcal{B}$ is a minimal partition of Ω, then G_B^B is primitive for each block $B \in \mathcal{B}$. For a G-invariant partition $\mathcal{B}$ of $V\Gamma$, the *quotient graph* $\Gamma_{\mathcal{B}}$ of Γ induced on $\mathcal{B}$ is the graph with vertex set $\mathcal{B}$ and B_i is adjacent in $\Gamma_{\mathcal{B}}$ to B_j if some $u \in B_i$ is adajcent in Γ to some $v \in B_j$. Two blocks $B, B' \in \mathcal{B}$ are said to be adjacent if they are adjacent in $\Gamma_{\mathcal{B}}$; denote by $\Gamma[B, B']$ the subgraph of Γ with vertex set $B \cup B'$ and with two verices adjacent if and only they are adjacent in Γ.

As in Theorem 1.1, let n be a positive square-free integer, and let Γ be an arc-transitive circulant of order n. We will complete the proof of Theorem 1.1 by proving the following proposition, which is slightly stronger than Theorem 1.1.

Proposition 2.1 *Let Γ be a G-arc-transitive circulant of square-free order, where $G \leq \mathrm{Aut}\Gamma$ and let R be a cyclic regular subgroup of G. Then one of the following statements holds.*

(1) *G is 2-transitive on $V\Gamma$, and Γ is a complete graph; or*

(2) *R is normal in G; or*

(3) *there exists a minimal G-invariant partition $\mathcal{B}$ of $V\Gamma$ such that for the kernel N of the G-action on $\mathcal{B}$ and for a block $B \in \mathcal{B}$, either*

   (i) *N is unfaithful on B and $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_b]$, or*

   (ii) *$K \cong K^B$ is 2-transitive on B and $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_b] - b\Gamma_{\mathcal{B}}$.*

The proof of this proposition consists of a series of lemmas. As in the proposition, we denote by G a subgroup of $\mathrm{Aut}\,\Gamma$ which is transitive on the set of arcs of Γ, and by R a cyclic subgroup of G. First, assume that G is primitive on $V\Gamma$. Then by Schur's Theorem (see [3, Theorem 3.5A, p. 95]), either G is 2-transitive, or $|V\Gamma| = p$ and $\mathbb{Z}_p \leq G \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$ for some prime p. Thus we have the following lemma.

Lemma 2.2 *If G is primitive on $V\Gamma$, then either Γ is complete, or R is normal in G.*

Hence we assume that G is imprimitive on $V\Gamma$ in the rest of this section.

Lemma 2.3 *Let $\mathcal{B}$ be a minimal G-invariant partition of $V\Gamma$, and let N be the kernel of the G-action on $\mathcal{B}$. Then either N^B is 2-transitive, or $\mathbb{Z}_p \leq N^B \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$, where $B \in \mathcal{B}$; in particular, in both cases N^B is primitive.*

Proof. It is clear that G_B^B is primitive, $N^B \lhd G_B^B$, and N contains the subgroup of R of order $|B|$. Thus N^B and so G_B^B contains a cyclic regular subgroup on B. By Schur's theorem, either G_B^B is 2-transitive, or $\mathbb{Z}_p \leq G_B^B \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$. By Burnside's theorem (see [3, Theorem 4.1B, p. 107]), if G_B^B is 2-transitive then $\mathrm{soc}(G_B^B)$ is nonabelian simple or elementary abelian. It then, follows since n is square-free, that either $T \leq G_B^B \leq \mathrm{Aut}(T)$ for some nonabelian simple group T, or $\mathbb{Z}_p \leq G_B^B \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$. If $\mathbb{Z}_p \leq G_B^B \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$, then we have $\mathbb{Z}_p \leq N^B \lhd G_B^B \leq \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$. Assume that $T \leq G_B^B \leq \mathrm{Aut}(T)$ with T nonabelian simple. Then T is transitive, and furthermore, N^B contains T. Suppose that N^B is imprimitive on B. Then there exists a N^B-invariant partition $\mathcal{B}'$ of B such that the regular cyclic subgroup (on B) of N^B is transitive and unfaithful on $\mathcal{B}'$. Thus N^B has a normal subgroup which is intransitive on B, which is not possible since T is the unique minimal normal subgroup of G_B^B and transitive on B. Hence N^B is primitive, and so 2-transitive. ■

Next we deal with two different cases according to the actions of N on a block $B \in \mathcal{B}$.

Lemma 2.4 *Assume that there exists a minimal G-invariant partition $\mathcal{B}$ of $V\Gamma$ such that N is unfaithful on B, where N is the kernel of the G-action on $\mathcal{B}$, and $B \in \mathcal{B}$. Then $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_b]$, where $b = |B|$; as in part* (3) (i).

Proof. Let M be the kernel of the N-action on B. Then $1 \neq M \lhd N$, and so $1 \neq M^{B'} \lhd N^{B'}$ for some $B' \in \mathcal{B}$. Since $N^{B'}$ is permutationally isomorphic to N^B and N^B is primitive (by Lemma 2.3), it follows that $M^{B'}$ is transitive on B'. As Γ is connected, there exists a sequence of blocks $B_0 = B, B_1, \ldots, B_l = B'$ such that a vertex in B_j is adjacent in Γ to some vertices in B_{j+1} for each $0 \leq j \leq l-1$, and there exists $0 \leq i < l$ such that $M^{B_j} = 1$ for all $j \leq i$ and $M^{B_{i+1}} \neq 1$. Then for $u \in B_i$, $M^{B_i \cup B_{i+1}}$ is transitive on $\{\{u, v\} \mid v \in B_{i+1}\}$. Since $N^{B_i \cup B_{i+1}}$ is transitive on B_i and fixes B_{i+1} (setwise), each vertex in B_i is adjacent to all vertices in B_{i+1}. It follows that $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_b]$, where $b = |B|$. ■

Lemma 2.5 *Assume that there exists a minimal G-invariant partition $\mathcal{B}$ of $V\Gamma$ such that $N \cong N^B$ is 2-transitive on B, where N is the kernel of G on $\mathcal{B}$, and $B \in \mathcal{B}$. Then $\Gamma = \Gamma_{\mathcal{B}}[\overline{K}_b] - b\Gamma_{\mathcal{B}}$, where $b = |B|$; as in part* (3) (ii).

Proof. We note that, since Γ is a circulant, we may label the vertices of Γ by elements of $\mathbb{Z}_n$, in such a way that $\Gamma = \mathrm{Cay}(R, S)$, where $S \subseteq \mathbb{Z}_n \setminus \{0\}$ satisfies $i \in S$ if and only if $n - i \in S$. The subset S will be called a *symbol* of Γ.

We are now going to distinguish two different cases, depending on whether the actions of the group N on the blocks in $\mathcal{B}$ are permutationally equivalent or not. (Recall that by [3, Lemma 1.6B, p.21] two transitive actions of a permutation group on two sets are equivalent if and only if the point stabilizer of the action on the first set coincides with the stabilizer of a point in the action on the second set.)

Case 1. The actions of N on the blocks in $\mathcal{B}$ are equivalent.

It follows that for each block $B' \in \mathcal{B}$, there exists $v' \in B'$ such that $N_{v'} = N_v$, where $v \in B$. Let $\mathrm{Equiv}(v)$ denote the collection of all such vertices v', that is $\mathrm{Equiv}(v) = \{v' \in V\Gamma \mid N_{v'} = N_v\}$. Then the 2-transitivity of the action of N on each of the blocks in $\mathcal{B}$ implies that the stabilizer N_v has two orbits in B', namely $\{v'\}$ and $B' \setminus \{v'\}$, or in other words, $B' \cap \mathrm{Equiv}(v)$ and $B' \setminus \mathrm{Equiv}(v)$. In particular, $|\mathrm{Equiv}(v) \cap B'| = 1$ for each $B' \in \mathcal{B}$.

Assume first that $\Gamma(v) \cap \mathrm{Equiv}(v) \neq \emptyset$, where $\Gamma(v)$ denotes the set of neighbors of v. Because of arc-transitivity we have that the bipartite graph induced by a pair of adjacent blocks is a perfect matching. Moreover, it may be seen that $\Gamma(v) \subseteq \mathrm{Equiv}(v)$. But $\mathrm{Equiv}(u) = \mathrm{Equiv}(v)$ for any $u \in \mathrm{Equiv}(v)$ and so the subgraph induced by the set $\mathrm{Equiv}(v)$ is a connected component of Γ, isomorphic to $\Gamma_{\mathcal{B}}$, a contradiction for Γ is connected and $b \neq 1$.

Assume now that $\Gamma(v) \cap \mathrm{Equiv}(v) = \emptyset$. Then for a block B' adjacent to B we must have that $\Gamma(v) \cap B' = B' \setminus \mathrm{Equiv}(v) = B' \setminus \{v'\}$. Let Γ' denote the graph obtained from Γ by joining two non-adjacent vertices of Γ if and only if they belong to two adjacent blocks in $\Gamma_{\mathcal{B}}$. In view of the comments of the previous paragraph $\Gamma' \cong b\Gamma_{\mathcal{B}}$ and so $\Gamma = \Gamma_{\mathcal{B}}[\overline{K_b}] - b\Gamma_{\mathcal{B}}$.

Case 2. The actions of N on the blocks in $\mathcal{B}$ are not (all) equivalent.

Using the classification of 2-transitive groups (see [3, Section 7.7]) we deduce that a 2-transitive group can have at most two inequivalent actions (of the same degree). Hence the set $\mathcal{B}$ decomposes into subsets $\mathcal{B}_0$ and $\mathcal{B}_1$ such that the actions of N on B and $B' \in \mathcal{B}$ are equivalent when $B' \in \mathcal{B}_0$ and inequivalent when $B' \in \mathcal{B}_1$. Moreover, in view of the fact that Γ is arc-transitive and thus the bipartite graphs induced by pairs of adjacent blocks are all isomorphic, it follows that $\{\mathcal{B}_0, \mathcal{B}_1\}$ is a bipartition of $V\Gamma_{\mathcal{B}}$ with $|\mathcal{B}_0| = |\mathcal{B}_1|$. In particular, $|\mathcal{B}| = m$ is an even number. Let ρ be a generator of the cyclic regular group R of G. Letting $B_i = B\,\rho^i$, we have that $\mathcal{B}_0$ consists of all the blocks B_i with $i \in \mathbb{Z}_m$ even and $\mathcal{B}_1$ consists of all the blocks B_i with $i \in \mathbb{Z}_m$ odd. Let $v_i^j = \rho^{i+mj}$, for all $i \in \mathbb{Z}_m$ and all $j \in \mathbb{Z}_b$.

Now the quotient graph $\Gamma_{\mathcal{B}}$ is a circulant. Assume that $2i+1$ belongs to the symbol of $\Gamma_{\mathcal{B}}$. (Note that the symbol of $\Gamma_{\mathcal{B}}$ contains only odd numbers.) Let $\sigma = \rho^{2i+1}$ and consider the blocks B_0, B_{2i+1} and B_{4i+2}. Let T be the subset of $\mathbb{Z}_b$ consisting of all those t such that $v = v_0^0$ is adjacent to v_{2i+1}^t. Then $v_{2i+1}^0 = v^\sigma$ is adjacent to $(v_{2i+1}^t)^\sigma = v^{\sigma\rho^{2i+1+mt}} = v^{\rho^{4i+2+mt}} = v_{4i+2}^t$, where $t \in T$. Therefore

$$v_{2i+1}^j \sim v_{4i+2}^l \iff l - j \in T. \tag{1}$$

Let $a \in \mathbb{Z}_b$ be such that $N_v = N_u$, where $u = v_{4i+2}^a$. Recall that the bipartite graphs induced by pairs of adjacent blocks are isomorphic, and moreover by the classification of 2-transtive groups [3, Section 7.7], N_v has two orbits of different cardinalities on B_{2i+1}. Hence u and v must have the same neighbors in B_{2i+1} and so $\Gamma(u) \cap B_{2i+1} = \{v_{2i+1}^t \mid t \in T\}$. Combining this together with (1) we have that $a - t \in T$ for each $t \in T$ and so

$$a - T = T. \tag{2}$$

Now because of the 2-transitivity of the action of N on each block, it follows that $|\Gamma(v_0^0) \cap \Gamma(v_0^j) \cap B_{2i+1}|$ is constant for all $j \in \mathbb{Z}_b \setminus \{0\}$. This implies the existence of a positive integer λ such that $|T \cap (T + j)| = \lambda$, for all $j \in \mathbb{Z}_b \setminus \{0\}$. Hence, in view of (2),

$$|T \cap (-T + a + j)| = \begin{cases} \lambda & \text{if } j \neq -a, \\ |T| & \text{if } j = -a. \end{cases} \tag{3}$$

We now make the following observation about the intersection $T \cap (-T + l)$. (See also [1, Lemma 2.1].) Whenever $x \in T \cap (-T + l)$ there must exist some $y \in T$ such that $x = -y + l$. Clearly, we get that $y \in T \cap (-T + l)$ by reversing the roles of x and y. So the elements in the intersection $T \cap (-T + l)$ are paired off with one exception occuring when $l \in 2T$. Then the equality $l = 2x$ ($x \in T$) gives rise to a unique element in the intersection $T \cap (-T+l)$. Therefore the parity of $|T \cap (-T+l)|$ depends solely on whether l belongs to $2T$ or not. More precisely, $|T \cap (-T+l)|$ is an odd number if $l \in 2T$ and an even number if $l \notin 2T$. Combining this fact with (3) we see that, in particular, $\mathbb{Z}_b \setminus \{-a\}$ is either a subset of $2T$ or of $\mathbb{Z}_b \setminus 2T$. But then in the first case $|T| = |2T| = b-1$ and in the second case $|T| = |2T| = 1$. In both case, a contradiction is derived with the assumption that the actions of N on B_0 and B_{2i+1} are inequivalent, completing the proof of Lemma 2.5. ■

Remark 2.6 Note that the bipartite graph arising from a pair of inequivalent 2-transitive group actions is the incidence graph of a symmetric block design with a 2-transitive automorphism group. (See [5] for the classification of all such designs.) Therefore the last part of the proof of Lemma2.5 thus amounted to proving that in an arc-transitive circulant of square-free order, the bipartite graph induced by two adjacent blocks cannot be the incidence graph of a symmetric design with the automorphism group acting 2-transitively on the sets of points and blocks of the design, respectively.

In view of the above lemmas, to complete the proof of Proposition 2.1, we may assume that

> *for each minimal G-invariant partition $\mathcal{X}$ of $V\Gamma$, letting F be the kernel of G on $\mathcal{X}$ and $X \in \mathcal{X}$, $F \cong F^X$ is not 2-transitive on X.*

Now let $\mathcal{B}$ be a minimal G-invariant partition of $V\Gamma$, and let N be the kernel of the G-action on $\mathcal{B}$. Take a block $B \in \mathcal{B}$. Then by Lemma 2.3,

$$\mathbb{Z}_p \leq N \cong N^B < \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1},$$

where p is a prime. Let $M = \mathrm{soc}(N)$, which is isomorphic to $\mathbb{Z}_p$. Then $M \lhd G$.

Lemma 2.7 *There is a subgroup H of $\mathbb{Z}_{p-1}$ and a group C such that $G = (M \times C).H$ and $M \leq R \leq M \times C$.*

Proof. Take $v \in V\Gamma$, and denote by G_v the stabilizer of v in G. Let P be a Sylow p-subgroup of G_v. Since n is square-free, $p|P|$ exactly divides $|G|$, and so $\langle M, P\rangle = M \rtimes P$ is a Sylow p-subgroup of G, that is, a Sylow p-subgroup of G is a split extension of M by P. By [7, Theorem 8.6, p. 232], G is a split extension of M by a subgroup L of G, where $L \cong G/M$, that is, $G = M \rtimes L$. Let $C = \mathbf{C}_L(M)$. Then $M \cap C = 1$, $C \lhd G$, and $G/(MC)$ is isomorphic to a subgroup of $\mathrm{Aut}(M)$ which is isomorphic to $\mathbb{Z}_{p-1}$. Thus $G = (M \times C).H$, where $H \leq \mathbb{Z}_{p-1}$. Since R is abelian and $M < R$, we have that $R < \mathbf{C}_G(M) = M \times C$. ■

We are now ready to complete the proof of Proposition 2.1.

Proof of Proposition 2.1. By Lemma 2.7, $G = (M_0 \times C_0).H_0$ such that $M_0 \leq R \leq M_0 \times C_0$ and $H_0 \leq \mathbb{Z}_{p_0-1}$, where p_0 is a prime. In particular, C_0 is normal in G and intransitive on $V\Gamma$. If $C_0 = 1$, then $R = M_0$ is normal in G, as required. Assume that $C_0 \neq 1$. Let $\mathcal{C}_1$ be the set of the C_0-orbits in $V\Gamma$. Then $\mathcal{C}_1$ is a G-invariant partition of $V\Gamma$. Let $\mathcal{B}^{(1)}$ be a minimal G-invariant partition of $V\Gamma$ which is a refined partition of $\mathcal{C}$. Take a block $B^{(1)} \in \mathcal{B}^{(1)}$. Let N_1 be the kernel of G on $\mathcal{B}^{(1)}$, and let $M_1 = \mathrm{soc}(N_1)$. By our assumption, N is faithful and is not 2-transitive on $B^{(1)}$. Then by Lemma 2.3, $M_1 \cong \mathbb{Z}_{p_1}$ for some prime p_1. By Lemma 2.7, $G = (M_1 \times C_1).H_1$ such that $M_1 \leq R \leq M_1 \times C_1$. Now $M_0 \times M_1 \leq R \leq (M_0 \times C_0) \cap (M_1 \times C_1)$. It follows that $R \leq (M_0 \times C_0) \cap (M_1 \times C_1) = M_0 \times M_1 \times C_1'$, and $G = (M_0 \times M_1 \times C_1').H_1'$. If $C_1' = 1$, then $R = M_0 \times M_1$ is normal in G, as required. Assume that $C_1' \neq 1$, and assume inductively that $G = (M_0 \times M_1 \times \ldots \times M_i \times C_i').H_i'$ such that $i \geq 1$, $\mathbb{Z}_{p_j} \cong M_j \leq R$ for each j, and $R \leq M_0 \times M_1 \times \ldots \times M_i \times C_i'$. Now C_i' is normal in G and intransitive on $V\Gamma$, and hence we may repeat our arguments with C_i' in place of C_0 so that we have $G = (M_{i+1} \times C_{i+1}).H_{i+1}$ such that $M_{i+1} \cong \mathbb{Z}_{p_{i+1}}$ for some prime p_{i+1}, and $M_{i+1} \leq R \leq M_{i+1} \times C_{i+1}$. Since $M_0, M_1, \ldots, M_{i+1} \leq R \leq (M_0 \times M_1 \times \ldots \times M_i \times C_i') \cap (M_{i+1} \times C_{i+1})$. It follows that $R \leq (M_0 \times M_1 \times \ldots \times M_i \times C_i') \cap (M_{i+1} \times C_{i+1}) = (M_0 \times M_1 \times \ldots \times M_{i+1} \times C_{i+1}')$ such that $G = (M_0 \times M_1 \times \ldots \times M_i \times M_{i+1} \times C_{i+1}').H_{i+1}'$. Therefore, repeating this argument, we finally obtain $G = (M_0 \times M_1 \times \ldots \times M_k).H$ such that $R = M_0 \times M_1 \times \ldots \times M_k$, which is normal in G, as required. ■

In view of the comments in the paragraph preceding the statement of Proposition 2.1, this completes the proof of Theorem 1.1.

References

[1] B. Alspach, M. D. E. Conder, D. Marušič, M.Y. Xu, A classification of 2-arc-transitive circulants, *J. Alg. Combin.*, **5** (1996), 83–86.

[2] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, London, New York, 1992.

[3] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York, 1996.

[4] C. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243-256.

[5] W. Kantor, Classification of 2-transitive symmetric designs, *Graphs Combin.* **1** (1985), 165–166.

[6] G. O. Sabidussi, Vertex-transitive graphs, *Monatsh. Math.* **68** (1964).

[7] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, New York, 1982.

Keywords: circulant graph, arc-transitive graph, square-free order, cyclic group, primitive group, imprimitive group.

CIRCULANTS OF SQUARE-FREE ORDER

Contact address:

Dragan Marušič

IMFM, Oddelek za matematiko

Univerza v Ljubljani

Jadranska 19, 1000 Ljubljana

Slovenija

tel. 386-61-1892320

fax 386-61-347997

email dragan.marusic@uni-lj.si