HALF-TRANSITIVE GRAPHS

by

Mateja Šajna

B.Sc., University of Ljubljana, 1992

Thesis submitted in partial fulfillment of
the requirements for the degree of

Master of Science

in the Department
of

Mathematics and Statistics

Simon Fraser University
July 1994

Approval

Name: Mateja Šajna

Degree: Master of Science

Title of Thesis: HALF-TRANSITIVE GRAPHS

Examining Committee:

Dr. Steve Thomason
Chair

Dr. Brian Alspach
Senior Supervisor

Dr. Luis Goddyn
Supervisor

Dr. Pavol Hell
Supervisor

Dr. Tom C. Brown
External Examiner

Date approved: July 13, 1994

Title of Thesis/Project/Extended Essay

HALF-TRANSITIVE GRAPHS

Author:

(signature)

(name)

1st June, 1994

(date)

Abstract

We explore the relation between vertex- and edge-transitivity and arc-transitivity of various graphs. We exhibit several families of graphs whose vertex- and edge-transitivity imply arc-transitivity. In particular, we show that any vertex- and edge-transitive graph with twice a prime number of vertices is arc-transitive by simplifying the proof of a theorem by Cheng and Oxley, in which they classify all vertex- and edge-transitive graphs of order twice a prime. A graph which is vertex- and edge-transitive but not arc-transitive is said to be $\frac{1}{2}$-transitive. We present Bouwer's construction, which yields one $\frac{1}{2}$-transitive graph for each even degree greater than 2, and exhibit several families of $\frac{1}{2}$-transitive metacirculants. In particular, we find a new family of $\frac{1}{2}$-transitive metacirculants with 4 blocks.

Acknowledgement

I wish to express my gratitude to Professor Brian Alspach for his encouragement, helpful suggestions, and careful proofreading. I would also like to thank Professors Luis Goddyn and Pavol Hell for their comments.

Contents

List of Figures

Chapter 1

Introduction

We begin with a set of definitions and known results from the theory of permutation groups. For any terms not defined here, the reader is referred to [19].

Let H be a permutation group acting on a finite set Ω. A set $\Delta \subseteq \Omega$ is a *fixed block* of H (or is *fixed setwise* by H) if $H(\Delta) = \Delta$, where $H(\Delta)$ denotes the set $\{g(\alpha) : g \in H, \alpha \in \Delta\}$. The *degree* of H is the number of points in Ω which are not fixed by H. Similarly, the *degree* of a permutation $g \in H$ is the number of points in Ω which are not fixed by g. A permutation group is *transitive* on Ω if it has only the trivial fixed blocks $\emptyset$ and Ω. A minimal fixed block of H other than $\emptyset$ is called an *orbit* of H. Thus any permutation group acts transitively on each of its orbits. It is easy to see that each point $\alpha \in \Omega$ lies in exactly one orbit of H, that is, $H(\alpha)$. Hence the orbits of H partition Ω. We thus have an equivalent definition of transitivity: a permutation group H is transitive on Ω if for any $\alpha, \beta \in \Omega$ there exists $g \in H$ such that $g(\alpha) = \beta$.

Let $S \subseteq \Omega$. The set $H_S = \{g \in H : g(\alpha) = \alpha \text{ for all } \alpha \in S\}$ is called the *stabilizer* of the set of points S and it is a subgroup of H. We write H_α for $H_{\{\alpha\}}$ and $H_{\alpha\beta}$ for $H_{\{\alpha,\beta\}}$. The following is a simple but very useful result.

Theorem 1.0.1 (Orbit-Stabilizer Theorem) *For any permutation group H acting on Ω and any $\alpha \in \Omega$,*

$$|H| = |H_\alpha| \cdot |H(\alpha)|.$$

PROOF. Since H_α is a subgroup of H, $|H| = |H_\alpha| \cdot |H : H_\alpha|$. Define a function $\sigma : H(\alpha) \to \{gH_\alpha : g \in H\}$ by $\sigma(\beta) = gH_\alpha$ if $g(\alpha) = \beta$. Since $g(\alpha) = h(\alpha)$ implies $h^{-1}g \in H_\alpha$ and hence $gH_\alpha = hH_\alpha$, σ is well-defined. If $\sigma(\beta) = \sigma(\gamma)$, then for $g, h \in H$ such that $g(\alpha) = \beta$ and $h(\alpha) = \gamma$, $gH_\alpha = hH_\alpha$. Hence $g(\alpha) = h(\alpha)$ and so $\beta = \gamma$. This proves that σ is a bijection. Therefore $|H(\alpha)| = |H : H_\alpha|$. $\square$

It follows from Theorem 1.0.1 that for any orbit Δ of H, the length $|\Delta|$ of Δ is a divisor of the order of H.

A permutation group H is called *regular* if it is transitive and if for each $\alpha \in \Omega$, $H_\alpha = 1$. By the Orbit-Stabilizer Theorem, a transitive permutation group H is regular if and only if $|H| = |\Omega|$, that is, if and only if its order and degree are equal. Notice also that in a regular group H, for any $\alpha, \beta \in \Omega$ there exists a unique $g \in H$ with $g(\alpha) = \beta$.

A *Frobenius group* is a transitive permutation group of degree n such that the minimum of degrees of elements $g \neq 1$ is $n - 1$. In other words, a Frobenius group H is a transitive non-regular group such that $H_{\alpha\beta} = 1$ for all $\alpha, \beta \in \Omega$, $\alpha \neq \beta$. The following non-trivial result is due to Frobenius (see [19]).

Theorem 1.0.2 *In a Frobenius group of degree n, the elements of degree n together with the identity form a regular group.*

A set $\Gamma \subseteq \Omega$ is a *block* of the permutation group H if for any $g \in H$, either $g(\Gamma) = \Gamma$ or $g(\Gamma) \cap \Gamma = \emptyset$. The sets $\emptyset$, Ω, and $\{\alpha\}$, for any $\alpha \in \Omega$, are the trivial blocks. A permutation group is *primitive* if it has no blocks other than the trivial ones; otherwise, it is *imprimitive.* It is easy to see that a primitive permutation group $H \neq \{1\}$ is transitive.

Proposition 1.0.3 *The length of a block of a transitive permutation group H divides the degree of H.*

PROOF. Let Γ be a block of a transitive permutation group H and let $g \in H$. We show that $g(\Gamma)$ is a block too. Take any $h \in H$ and let $u = g^{-1}hg$. If $h(g(\Gamma)) \cap g(\Gamma) \neq$

$\emptyset$, then $gu(\Gamma) \cap g(\Gamma) \neq \emptyset$ and so $u(\Gamma) \cap \Gamma \neq \emptyset$. Since Γ is a block, this implies $u(\Gamma) = \Gamma$. Thus $h(g(\Gamma)) = g(\Gamma)$ and so $g(\Gamma)$ is a block. Since H is transitive, $\{g(\Gamma) : g \in H\}$ is a partition of Ω into blocks of the same length. Thus $|\Gamma|$ divides $|\Omega|$. $\square$

We immediately have

Corollary 1.0.4 *A transitive permutation group of prime degree is primitive.*

A permutation group H is 2-*transitive* (or *doubly transitive*) if for any α_1, α_2, β_1, and β_2 in Ω with $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, there exists $g \in H$ such that $g(\alpha_i) = \beta_i$ for $i = 1, 2$. It is easy to see that a transitive permutation group H is 2-transitive on Ω if and only if H_α is transitive on $\Omega - \alpha$ for some $\alpha \in \Omega$. It can be shown that every 2-transitive permutation group is primitive. The converse is not true. However, Liebeck and Saxl [9] have proved the following.

Theorem 1.0.5 *Let p be a prime. A primitive permutation group of degree $2p$ is doubly transitive provided that $p \neq 5$. The only primitive groups of degree 10 which are not doubly transitive are the symmetric group S_5 and the alternating group A_5 acting on the set of 2-element subsets of a 5-element set.*

This result will be a crucial point in the proof of Theorem 2.1.7. In the same proof, we shall be heavily using the next result due to Burnside (see [14], p. 53), which gives a nice description of transitive permutation groups of prime degree in terms of affine linear transformations of Z_p.

Theorem 1.0.6 *Let H be a transitive permutation group acting on a p-element set Ω, where p is a prime. Then either H is doubly transitive or we can identify Ω with Z_p such that*

$$\{x + b : b \in Z_p\} \subseteq H \subset \{ax + b : a \in Z_p^*, b \in Z_p\}.$$

Now let H be a transitive but not doubly transitive permutation group acting on Ω, and let $\alpha \in \Omega$. Then H_α is not transitive on $\Omega - \alpha$. Let $\Delta \subseteq \Omega - \alpha$ be an orbit of H_α. Define Δ' by

$$\Delta' = \{g(\alpha) : g \in H \text{ such that } \alpha \in g(\Delta)\}.$$

It can be shown that Δ' is also an orbit of H_α, that $(\Delta')' = \Delta$, and that $|\Delta'| = |\Delta|$. The orbits Δ and Δ' are called *paired orbits* of H_α.

The following result together with Theorem 1.0.2 will be used in proving Theorem 2.1.10 (see [19]).

Theorem 1.0.7 *Let H be a primitive but not doubly transitive permutation group. If H_α has an orbit Δ with length 2, then H is a Frobenius group and it contains a regular normal subgroup of index 2.*

We continue with some graph-theoretic preliminaries. Any terms not defined here can be found in [4].

The complete graph on n vertices, the n-cycle, and the path with n vertices will be denoted by K_n, C_n, and P_n, respectively. $K_{m,n}$ denotes the complete bipartite graph with vertex classes of sizes m and n, respectively. The disjoint union of the graphs G_1 and G_2 is denoted by $G_1 + G_2$. G^c is the complement of the graph G and $N(x)$ is the set of neighbours of the vertex x in the given graph. K_n^c is called the *edgeless graph* on n vertices. Adjacency in the given graph is denoted by $\sim$.

Let $G = (V, E)$ be a graph with vertex set V and edge set E. The set of *arcs* of G is $A(G) = \{(u, v) : uv \in E\}$. G is said to be *vertex-transitive, edge-transitive*, and *arc-transitive* (or *1-transitive*) if its automorphism group $\mathrm{Aut}(G)$ acts transitively on the vertices, edges, and arcs of G, respectively. Clearly, arc-transitivity implies edge-transitivity. However, there exist edge-transitive graphs which are not arc-transitive, vertex-transitive graphs which are not edge-transitive and edge-transitive graphs which are not vertex-transitive. The objective of this thesis is to explore the relation between vertex- and edge-transitivity and arc-transitivity of various graphs. In Chapter 2 we exhibit several families of graphs whose vertex- and edge-transitivity imply arc-transitivity and in the much longer Chapter 3 we talk about graphs which are vertex- and edge-transitive but not arc-transitive. Such graphs are called $\frac{1}{2}$-*transitive* or *half-transitive*. The study of this topic started with Tutte [16] in 1966 and Bouwer [5] in 1970.

Let Γ be a group and let $\Delta \subseteq \Gamma$ be such that $1 \notin \Delta = \Delta^{-1}$, where $\Delta^{-1} = \{\delta^{-1} : \delta \in \Delta\}$. The *Cayley graph* $K(\Gamma, \Delta)$ has vertex set Γ and edge set $\{x\,(x\delta) : x \in \Gamma, \delta \in \Delta\}$. A *circulant graph* $C(n; S)$ is a graph with vertex set $\{u_0, u_1, \ldots, u_{n-1}\}$ and u_i adjacent to u_j if and only if $j - i \in S$, where $S \subseteq Z_n$ and $S = -S = \{(-s) \bmod n : s \in S\}$. In other words, a circulant graph is a Cayley graph on a cyclic group. The following result is well-known.

Theorem 1.0.8 *A graph with a prime number of vertices is vertex-transitive if and only if it is a circulant graph.*

PROOF. It is obvious that a circulant graph is vertex-transitive. Now let G be a vertex-transitive graph of order p, where p is a prime. By the Orbit-Stabilizer Theorem, $|\mathrm{Aut}(G)|$ is divisible by p. Hence $\mathrm{Aut}(G)$ contains an element ρ of order p. Since ρ is acting on p vertices, it must be a p-cycle $(u_0\ u_1\ \ldots\ u_{n-1})$. It is then easy to see that we can determine the symbol S of G using ρ. $\square$

The following can be shown by elementary group theory (see [7], p. 49).

Proposition 1.0.9 *Every group of order p^2, where p is a prime, is abelian.*

This statement, together with the next result due to Marušič [11], will be used in proving Corollary 2.1.5.

Proposition 1.0.10 *Every vertex-transitive graph of order p^2, where p is a prime, is a Cayley graph on a group of order p^2.*

We conclude with several observations of a number-theoretic nature.

For any positive integer $n \geq 2$, Z_n is a commutative ring with identity 1. The set Z_n^* of units of Z_n is a multiplicative group of order $\varphi(n)$, where φ is the Euler φ-function. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers, then

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \ldots (p_k - 1)p_k^{\alpha_k - 1}.$$

The following can be said about the structure of Z_n^* (see [3]).

Theorem 1.0.11 *The multiplicative group Z_n^* is cyclic if and only if $n = 2$, $n = 4$, n is an odd prime power, or n is twice an odd prime power. If $n = n_1 n_2$ where n_1 and n_2 are relatively prime, then Z_n^* is isomorphic to the direct product $Z_{n_1}^* \times Z_{n_2}^*$.*

And finally, a famous theorem of Dirichlet's (again, see [3]).

Theorem 1.0.12 *An arithmetic progression of numbers of the form $ak + b$ contains infinitely many primes whenever $a \neq 0$ and* $\gcd(a, b) = 1$.

Chapter 2

When vertex- and edge-transitivity imply arc-transitivity

2.1 Graphs whose vertex- and edge-transitivity imply arc-transitivity

The following lemma will be used frequently to establish the arc-transitivity of various graphs.

Lemma 2.1.1 *Let G be a vertex-transitive graph having a vertex x such that for any $y, y' \in N(x)$ there exists an automorphism of G that fixes x and maps y to y'. Then G is arc-transitive.*

PROOF. Take any two edges uv, $u'v'$ in G. Since G is vertex-transitive, there exist $g, h \in \mathrm{Aut}(G)$ such that $g(u) = x$ and $h(u') = x$. Let $y = g(v)$ and $y' = h(v')$. Let $f \in \mathrm{Aut}(G)$ be such that $f(x) = x$ and $f(y) = y'$. Such an automorphism exists by the assumption of the lemma. We now have $h^{-1}fg(u) = u'$ and $h^{-1}fg(v) = v'$. Since uv and $u'v'$ were arbitrary, G is arc-transitive. □

The first result concerning graphs whose vertex- and edge-transitivity force the graph to be arc-transitive is due to Tutte [16]. The combinatorial proof we present here was given by Cheng and Oxley [6].

Proposition 2.1.2 *Let G be a vertex- and edge-transitive graph of degree r where r is odd. Then G is arc-transitive.*

PROOF. Evidently, if G has an automorphism that interchanges the endpoints of an edge, then, since G is edge-transitive, G is arc-transitive. Assume that G is not arc-transitive and fix an edge e of G. Assign a direction to e. Then, for each edge f distinct from e, there is an automorphism mapping e to f and hence inducing a direction on f. If there are two such automorphisms σ_1 and σ_2 inducing different directions on f, then $\sigma_1\sigma_2^{-1}$ fixes the edge f and interchanges its endpoints - a contradiction. It follows that we obtain a directed graph $\mathbf{G}$ such that $\mathrm{Aut}(G) \subseteq \mathrm{Aut}(\mathbf{G})$. Since G is vertex-transitive, the indegrees of all vertices of $\mathbf{G}$ are the same. Likewise, all the outdegrees are the same. But since the sum of the indegrees equals the sum of the outdegrees, each vertex has its indegree and outdegree equal. Thus G has even degree - a contradiction. □

The next result appears in [2] and has several consequences. The assertions of Corollaries 2.1.4 and 2.1.5 are mentioned in [2] whereas Corollary 2.1.6 is new.

Proposition 2.1.3 *Every vertex- and edge-transitive Cayley graph on an abelian group is also arc-transitive.*

PROOF. Let $G = K(\Gamma, \Delta)$ be an edge-transitive Cayley graph on an abelian group Γ. Define $\sigma : \Gamma \rightarrow \Gamma$ by $\sigma(x) = x^{-1}$ for all $x \in \Gamma$. Then, since Γ is abelian and since $\Delta^{-1} = \Delta$, σ maps any edge $\{x, x\delta\}$ onto the edge $\{x^{-1}, x^{-1}\delta^{-1}\}$ so that σ is an automorphism of G. For any $g \in \Gamma$, let μ_g be the automorphism of G defined by $\mu_g(x) = gx$. Then $\mu_\delta\sigma$ interchanges the endpoints of the edge $\{1, \delta\}$. Consequently, G is arc-transitive. □

Corollary 2.1.4 *Every vertex- and edge-transitive graph of order p, where p is a prime, is arc-transitive.*

PROOF. Let G be a vertex- and edge-transitive graph on a prime number of vertices. Then, by Theorem 1.0.8, G is a circulant graph, that is, a Cayley graph on a cyclic, and hence abelian, group. The result now follows by Proposition 2.1.3. $\square$

Corollary 2.1.5 *Every vertex- and edge-transitive graph of order p^2, where p is a prime, is arc-transitive.*

PROOF. This follows immediately from Propositions 1.0.10, 1.0.9, and 2.1.3. $\square$

Corollary 2.1.6 *Every edge-transitive Cayley graph on a dihedral group is arc-transitive.*

PROOF. Let $G = K(\Gamma, \Delta)$ be an edge-transitive Cayley graph on a dihedral group Γ. If Δ contains an element δ of order 2, then $\mu_\delta(x) = \delta x$ interchanges the end-points of the edge $\{1, \delta\}$ and so G is arc-transitive. Otherwise, G consists of two disjoint isomorphic subgraphs which are Cayley graphs on a cyclic group. Hence by Proposition 2.1.3, G is arc-transitive. $\square$

The following result has been proved by Cheng and Oxley in [6]. The proof is rather long and will be worked out in full detail in section 2.2.

Theorem 2.1.7 *Every vertex- and edge-transitive graph of order $2p$, where p is a prime, is arc-transitive.*

In [2], Alspach, Marušič, and Nowitz have shown the following.

Theorem 2.1.8 *Every vertex- and edge-transitive graph of order less than 27 is arc-transitive.*

PROOF. If there exists a $\frac{1}{2}$-transitive graph of order $n < 27$, then by Corollaries 2.1.4 and 2.1.5, and by Theorem 2.1.7, $n \in \{8, 12, 15, 16, 18, 20, 21, 24\}$. McKay [12] has published a list of all vertex-transitive graphs with 19 or fewer vertices. He also included information about the orders of vertex-stabilizers and automorphisms that interchange the endvertices of an edge. This additional information eliminates all but thirteen graphs, none of which is edge-transitive. Vertex-transitive graphs with 20 and 21 vertices, amongst others, have been catalogued by McKay and Royle [13]. None of them are $\frac{1}{2}$-transitive. Finally, Praeger and Royle [15] have shown that every vertex- and edge-transitive graph with 24 vertices is also arc-transitive. Hence there is no $\frac{1}{2}$-transitive graph of order less than 27. $\square$

The last result we present in this section is due to Yu [18]. But first we need a lemma.

Lemma 2.1.9 *Let G be a $\frac{1}{2}$-transitive graph. Then for any $u \in V(G)$ and any $v \in N(u)$, $N(u)$ is the disjoint union of Δ_v and Δ'_v, where Δ_v is the orbit of $\mathrm{Aut}(G)_u$ containing v, and Δ'_v is the paired orbit of $\mathrm{Aut}(G)_u$.*

PROOF. Since G is not arc-transitive, by Lemma 2.1.1, $Aut(G)_u$ is not transitive on $N(u)$. Thus $\Delta_v \neq N(u)$. Obviously, $\Delta_v \subseteq N(u)$ and, by the definition of a paired orbit (see page 4), $\Delta'_v \subseteq N(u)$. For any $x \in N(u)$ there exists $g \in \mathrm{Aut}(G)$ such that $g(\{u,v\}) = \{u,x\}$. If $g(u) = u$, then $g(v) = x$ so that $x \in \Delta_v$. If $g(u) = x$, then $g(v) = u$ so that $g(u) = x \in \Delta'_v$. Hence $N(u) = \Delta_v \cup \Delta'_v$. Suppose that $\Delta_v = \Delta'_v$. Choose $f \in \mathrm{Aut}(G)$ with $f(v) = u$. Since $\Delta_v = \Delta'_v$, $f(u) \in \Delta_v$. Since $v \in \Delta_v$, there exists $h \in \mathrm{Aut}(G)_u$ such that $h(f(u)) = v$. But then hf interchanges u and v, a contradiction. Hence $N(u)$ is the disjoint union of Δ_v and Δ'_v. $\square$

Theorem 2.1.10 *Let G be a vertex- and edge-transitive graph of degree 4. If $\mathrm{Aut}(G)$ is primitive on $V(G)$, then G is arc-transitive.*

PROOF. Suppose that G is a $\frac{1}{2}$-transitive graph of degree 4 such that $\Gamma = \mathrm{Aut}(G)$ is primitive on $V(G)$. By Lemma 2.1.9, for any $u \in V(G)$ and any $v \in N(u)$, $N(u)$ is the disjoint union of Δ_v and Δ'_v. Since $|N(u)| = 4$ and since paired orbits have the same length, $|\Delta_v| = 2$ so that Γ_u has an orbit of length 2. Then by Theorem 1.0.7, Γ is a Frobenius group. Since

$$|\Gamma| = |\Gamma_u|\,|\Gamma(u)| = |\Gamma_{uv}|\,|\Gamma_u(v)|\,|\Gamma(u)|$$

and since $|\Gamma_{uv}| = 1$ for a Frobenius group,

$$|\Gamma| = |\Gamma_u(v)|\,|\Gamma(u)| = |\Delta_v| \cdot n = 2n,$$

where $n = |V(G)|$. Hence $|\Gamma_u| = 2$ and so there are exactly two automorphisms of G that fix u; one of them is the identity and the other has order 2. Since every element of a Frobenius group (other than the identity) has degree at least $n-1$, any $g \in \Gamma - \{1\}$ that fixes a point has the cyclic decomposition

$$g = (i_1\, j_1)(i_2\, j_2)\ldots(i_k\, j_k)$$

where $n = 2k+1$. If g and h are distinct automorphisms of this form, then they have no transpositions in common since otherwise $gh \neq 1$ would fix two vertices. Hence every transposition occurs at most once in the cyclic decompositions of the elements of degree $n-1$. By Theorems 1.0.2 and 1.0.7, the elements of degree n together with the identity form a regular normal subgroup of index 2 in Γ. Hence Γ contains $\frac{|\Gamma|}{2} = n$ automorphisms of degree $n-1$. Thus the number of distinct transpositions contained in automorphisms of degree $n-1$ is $\frac{n-1}{2} \cdot n = \binom{n}{2}$. Therefore, for any two vertices u and v, we can find an automorphism that interchanges u and v, contradicting the assumption that G is $\frac{1}{2}$-transitive. □

2.2 Vertex- and edge-transitive graphs of order twice a prime

In [6], Cheng and Oxley have characterized all vertex- and edge-transitive graphs of order twice a prime. As a by-product, their characterization shows that these graphs are all arc-transitive. The aim of this section is to prove only this by-product. We shall therefore follow the argument of [6] taking shortcuts whenever possible. Thus we shall avoid the use of the characterization of finite simple groups. Lemma 2.2.4, however, is new; its proof is based on the proof of Lemma 6.1 and a part of the proof of Theorem 6.2 in [10]. This lemma could also be used in the proof of Cheng and Oxley to avoid introducing group characters.

Throughout this section let G be a vertex- and edge-transitive graph of order $2p$, where p is a prime. Because of Proposition 2.1.2, we may assume G has even degree.

When $p = 2$, G is either the edgeless graph $(K_4)^c$ or C_4 and both are arc-transitive. The regular graphs of order 6 and of even degree are the edgeless graph $(K_6)^c$, $2K_3$, C_6, and $(3K_2)^c$. They are all arc-transitive. We may therefore assume that $p \geq 5$.

By Theorem 1.0.5, either $\mathrm{Aut}(G)$ is doubly transitive, $\mathrm{Aut}(G)$ is imprimitive, or $\mathrm{Aut}(G)$ is primitive but not doubly transitive and $p = 5$. In the first case, G is either the edgeless graph $(K_{2p})^c$ or the complete graph K_{2p} and hence arc-transitive. In the last case we recall that the only primitive groups of degree 10 which are not doubly transitive are S_5 and A_5 acting on the set $V = \{\{a,b\} : a,b \in Z_5, a \neq b\}$. Let G be a vertex- and edge-transitive graph with $V(G) = V$ whose automorphism group is either S_5 or A_5 acting on V. Since G is edge-transitive, for every pair of adjacent vertices $\{a,b\}$ and $\{c,d\}$, $|\{a,b\} \cap \{c,d\}|$ is the same. If this number is 0, then G is the Petersen graph; if it is 1, G is the complement of the Petersen graph. Both graphs are well known to be arc-transitive.

For the rest of the proof we shall assume that $\mathrm{Aut}(G)$ is imprimitive. Thus $\mathrm{Aut}(G)$ has a block containing p vertices or a block containing 2 vertices. We treat these two cases separately. The next two lemmas, however, will be used in both cases.

Lemma 2.2.1 *The graph G has the property that either no edge joins two vertices in different blocks of* $\mathrm{Aut}(G)$*, or no edge joins two vertices in the same block of* $\mathrm{Aut}(G)$.

PROOF. This follows immediately from the definition of a block using the fact that G is edge-transitive. $\square$

Lemma 2.2.2 *Suppose that the graph G is bipartite having as its vertex classes two disjoint copies, $\{0, 1, \ldots, p-1\}$ and $\{0', 1', \ldots, (p-1)'\}$, of Z_p. If G has an automorphism τ which, for all $i \in Z_p$, maps i to $i+1$ and i' to $(i+1)'$, then G is arc-transitive.*

PROOF. Consider the permutation ρ of $V(G)$ which, for all $i \in Z_p$, maps i to $(-i)'$ and i' to $-i$. If $ij' \in E(G)$, then so is $\rho(ij')$ since $\rho(ij') = (-i)'(-j) = \tau^{-i-j}(j'i)$. Thus ρ is an automorphism of G. By Lemma 2.1.1, since G is vertex-transitive, it is enough to show that for any elements i' and j' of $N(0)$, there is an automorphism fixing 0 and mapping i' to j'. Since G is edge-transitive, it certainly has an automorphism μ that maps $\{0, i'\}$ to $\{0, j'\}$. If μ fixes 0, μ is the required automorphism. We therefore suppose that μ maps 0 to j' and i' to 0. But then the automorphism $\rho\tau^{-j}\mu$ has the desired effect. $\square$

The following lemma settles the case when $\mathrm{Aut}(G)$ has a block of size p.

Lemma 2.2.3 *If G is a vertex- and edge-transitive graph of order $2p$, where p is an odd prime, such that $\mathrm{Aut}(G)$ has a block of size p, then G is arc-transitive.*

PROOF. Let A be a block of $\mathrm{Aut}(G)$ of size p. Then $V(G) - A$ is also a block of $\mathrm{Aut}(G)$ and we denote it by A'.

Suppose that G has an edge that joins two vertices in A or joins two vertices in A'. Then by Lemma 2.2.1, there is no edge with one endpoint in A and the other endpoint in A' so that G is disconnected. The induced subgraphs $G[A]$ and $G[A']$ are vertex- and edge-transitive graphs on a prime number of vertices, hence, by Corollary 2.1.4, they are arc-transitive. Consequently, G is arc-transitive.

We may therefore assume that G is a bipartite graph having A and A' as its vertex classes. If G is the complete bipartite graph $K_{p,p}$, then G is arc-transitive. Hence we may assume that this is not the case.

Since G is vertex-transitive, by the Orbit-Stabilizer Theorem, $|\mathrm{Aut}(G)|$ is divisible by p. Hence G has an automorphism π of order p. As p is odd, $\pi(A) = A$ and $\pi(A') = A'$. Denote $\pi_1 = \pi|_A$ and $\pi_2 = \pi|_{A'}$. Suppose that $\pi_2 = 1$. Then π_1 is a p-cycle. From this it follows that every vertex in A' is adjacent to every vertex in A so that G is isomorphic to $K_{p,p}$ - a contradiction. Similarly, we may assume that $\pi_1 \neq 1$.

Thus $\pi = \pi_1\pi_2$ where π_1 and π_2 are disjoint p-cycles. Evidently, A and A' may be identified with distinct copies, $\{0, 1, \ldots, p-1\}$ and $\{0', 1', \ldots, (p-1)'\}$, of Z_p. Moreover, these identifications can be made in such a way that the automorphism π found above maps i to $i+1$ and i' to $(i+1)'$ for all $i \in Z_p$. It now follows from Lemma 2.2.2 that G is arc-transitive. □

For the rest of the section we assume that G is a vertex- and edge-transitive graph of order $2p$ such that $\mathrm{Aut}(G)$ has a block A_0 of size 2 but no blocks of size p. As $\mathrm{Aut}(G)$ is transitive on $V(G)$, by the Orbit-Stabilizer Theorem, there is an automorphism τ of G of order p. Moreover, A_0, $\tau(A_0)$, $\tau^2(A_0), \ldots, \tau^{p-1}(A_0)$ are distinct blocks of $\mathrm{Aut}(G)$. For convenience, we shall denote these blocks by $A_0, A_1, \ldots, A_{p-1}$, where, for $i \in Z_p$, $A_i = \{i, i'\}$ and τ maps i to $i+1$ and i' to $(i+1)'$. As before, we denote the sets $\{0, 1, \ldots, p-1\}$ and $\{0', 1', \ldots, (p-1)'\}$ by A and A', respectively.

We first note that, by Lemma 2.2.1, if G has an edge ii' for some $i \in Z_p$, then G is isomorphic to pK_2 and hence G is arc-transitive. We may therefore assume that, for all $i \in Z_p$, ii' is not an edge of G.

Let $\overline{G}$ be the graph induced by G on the blocks of $\mathrm{Aut}(G)$. Thus $\overline{G}$ has vertex-set $\{\overline{i} : i \in Z_p\}$ and edge-set $\{\overline{i}\,\overline{j} : G$ has an edge between blocks A_i and $A_j\}$. If $\theta \in \mathrm{Aut}(G)$, then θ induces an automorphism $\overline{\theta}$ on $\overline{G}$. Thus the map from $\mathrm{Aut}(G)$ to $\mathrm{Aut}(\overline{G})$ that sends θ to $\overline{\theta}$ is a group homomorphism. Let $\overline{\mathrm{Aut}(G)}$ be the image of $\mathrm{Aut}(G)$ under this homomorphism. Evidently $\overline{\mathrm{Aut}(G)}$ acts transitively on both $V(\overline{G})$ and $E(\overline{G})$ and so $\overline{G}$ is a vertex- and edge-transitive graph of order p. By Corollary 2.1.4, $\mathrm{Aut}(\overline{G})$ acts transitively on the arcs of $\overline{G}$ as well.

Next we consider the number $e(A_i, A_j)$ of edges of G between the blocks A_i and A_j of $\mathrm{Aut}(G)$. Clearly $0 \le e(A_i, A_j) \le 4$. Since G is edge-transitive, for all pairs of adjacent blocks A_i and A_j, $e(A_i, A_j)$ takes the same value which we denote by $e(G)$.

For any pair A_i and A_j of blocks of $\mathrm{Aut}(G)$, the subgraph $G[A_i, A_j]$ induced by $A_i \cup A_j$ is bipartite and edge-transitive. No such graph has exactly 3 edges so that $e(G) \neq 3$.

If $e(G) = 4$, then $G[A_i, A_j] \cong K_{2,2}$ for each pair of adjacent blocks A_i and A_j. Consequently, each automorphism of $\overline{G}$ is induced by an automorphism of G. Since $\overline{G}$ is arc-transitive, it follows that G is too.

From now on we may assume that either $e(G) = 1$ or $e(G) = 2$. Now $\overline{\mathrm{Aut}(G)}$ acts transitively on $V(\overline{G})$, thus it may in fact act doubly transitively on $V(\overline{G})$. The next lemma shows that this does not happen.

Lemma 2.2.4 *Let G be a vertex- and edge-transitive graph of order $2p$, where p is an odd prime. Suppose $\mathrm{Aut}(G)$ has a block of size 2 but no block of size p, and that $e(G) \in \{1, 2\}$, where $e(G)$ denotes the number of edges between two adjacent blocks of size 2 in G. Then $\overline{\mathrm{Aut}(G)}$ does not act doubly transitively on $V(\overline{G})$.*

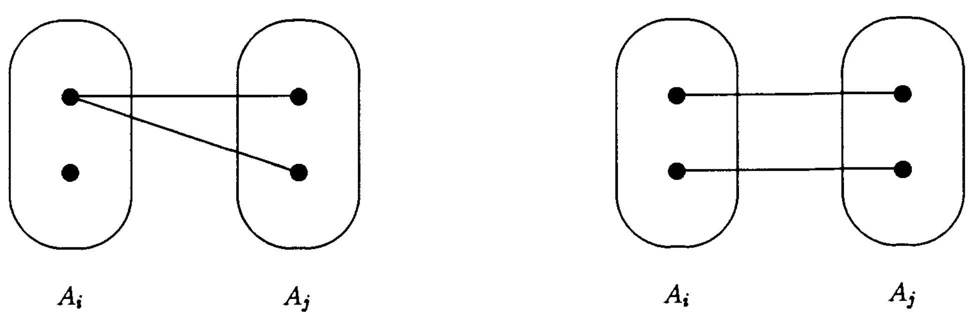

Figure 2.1: Lemma 2.2.4, Case 1 and Case 2

PROOF. Let G satisfy the assumptions of the lemma and suppose that $\overline{\mathrm{Aut}(G)}$ is doubly transitive. Then $\overline{G}$ is a complete graph and the subgraphs $G[A_i, A_j]$ of G, for any two blocks A_i and A_j, are all isomorphic. According to what the graphs $G[A_i, A_j]$ are, there are three possibilities. We will show that none of them actually occurs.

Case 1. $G[A_i, A_j] \cong P_3 + K_1$ for all $i, j \in Z_p$, $i \neq j$.
Since $\overline{\mathrm{Aut}(G)}$ is doubly transitive, there exists $\theta \in \mathrm{Aut}(G)$ that interchanges the blocks A_i and A_j, contradicting the structure of the graph $G[A_i, A_j]$.

Case 2. $G[A_i, A_j] \cong 2K_2$ for all $i, j \in Z_p$, $i \neq j$.
Define the sets $S = \{k \in Z_p^* : k \sim 0\}$ and $T = \{k \in Z_p^* : k' \sim 0\}$. Notice that, because of the structure of the graphs $G[A_i, A_j]$, $k \sim 0$ if and only if $k' \sim 0'$ and $k' \sim 0$ if and only if $k \sim 0'$. Also, using the automorphism τ of G, we can see that $i \sim i + r$ if and only if $r \in S$, $i' \sim (i + r)'$ if and only if $r \in S$, $i \sim (i + r)'$ if and only if $r \in T$, and $i' \sim i + r$ if and only if $r \in T$. The sets S and T have the following properties: $S = -S$, $T = -T$, $S \cap T = \emptyset$, and $S \cup T = Z_p^*$ since $\overline{G}$ is complete. For $r \in Z_p^*$, let $S + r$ denote the set $\{k + r : k \in S\}$. We define $T + r$ similarly.

It follows from the properties listed above that

$$|(T + r) \cap S| = |-(T + r) \cap (-S)| = |(T - r) \cap S| = |T \cap (S + r)|.$$

By the definitions of the sets S and T,

$$i + k \in N(i) \cap N(i + r) \text{ if and only if } k \in S \cap (S + r)$$

and

$$(i + k)' \in N(i) \cap N(i + r) \text{ if and only if } k \in T \cap (T + r).$$

For any $i \in Z_p$, $r \in Z_p^*$ we thus have

$$\begin{aligned}
|N(i) \cap N(i + r)| &= |S \cap (S + r)| + |T \cap (T + r)| \\
&= |S \cap (Z_p^* + r)| - |S \cap (T + r)| + |T \cap (Z_p^* + r)| - |T \cap (S + r)| \\
&= |Z_p^* \cap (Z_p^* + r)| - 2|S \cap (T + r)| \\
&= p - 2 - 2|S \cap (T + r)|
\end{aligned}$$

so that $|N(i) \cap N(i + r)|$ is odd for any $i \in Z_p$, $r \in Z_p^*$.

Similarly,

$$i + k \in N(i') \cap N(i + r) \text{ if and only if } k \in T \cap (S + r)$$

and

$$(i + k)' \in N(i') \cap N(i + r) \text{ if and only if } k \in S \cap (T + r),$$

which implies

$$\begin{aligned} |N(i') \cap N(i + r)| &= |T \cap (S + r)| + |S \cap (T + r)| \\ &= 2|S \cap (T + r)| \end{aligned}$$

so that $|N(i') \cap N(i + r)|$ is even for any $i \in Z_p$, $r \in Z_p^*$.

Now, if A and A' are not blocks of $\mathrm{Aut}(G)$, then there exist $\theta \in \mathrm{Aut}(G)$, $i, j, k \in A$ and $l' \in A'$ such that $\theta(i) = j$ and $\theta(k) = l'$. But then we must have $|N(i) \cap N(k)| = |N(j) \cap N(l')|$, which is impossible since $|N(i) \cap N(k)|$ is odd and $|N(j) \cap N(l')|$ is even. Hence $\mathrm{Aut}(G)$ has a block of size p, contradicting the assumption of the Lemma.

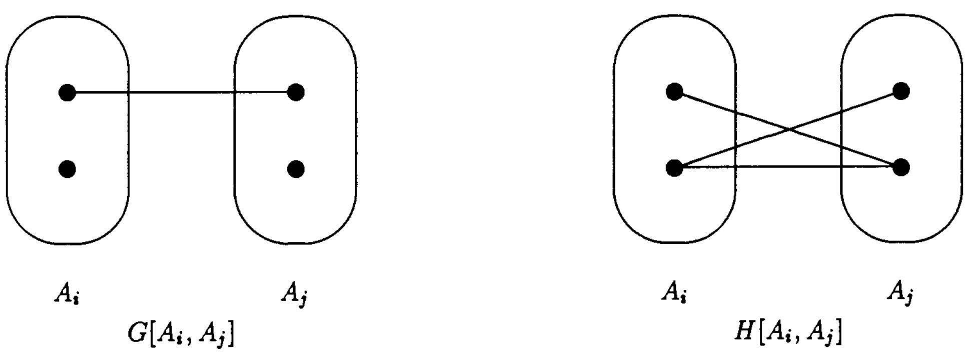

Figure 2.2: Lemma 2.2.4, Case 3

Case 3. $G[A_i, A_j] \cong K_2 + 2K_1$ for all $i, j \in Z_p$, $i \neq j$.
Let H be the graph with $V(H) = V(G)$ such that for all $i, j \in Z_p$, $i \neq j$, the subgraph $H[A_i, A_j]$ of H induced by $A_i \cup A_j$ is the bipartite complement of $G[A_i, A_j]$. Thus $H[A_i, A_j] \cong P_4$. Notice, also, that $\mathrm{Aut}(G) \subseteq \mathrm{Aut}(H)$.

Let (A_i, A_j) and (A_k, A_l) be two pairs of distinct 2-blocks of Aut(G). Since $\overline{\text{Aut}(G)}$ is doubly transitive on the vertices of $\overline{G} = \overline{H}$, we can map an end-edge of the path $H[A_i, A_j]$ to any of the two end-edges of the path $H[A_k, A_l]$, but it is impossible to map it to the central edge of the path $H[A_k, A_l]$. Hence there exists an edge orbit $Q \subset E(H)$ of Aut(H) such that for the subgraph $H[Q]$ of H induced by Q, $H[Q] \cap H[A_i, A_j] \cong 2K_2$ for any $i, j \in Z_p$, $i \neq j$. Now, to the graph $H[Q]$ we can apply the procedure of Case 2 to show that Aut$(H[Q])$ has blocks of size p. Since Aut$(G) \subseteq$ Aut$(H) \subseteq$ Aut$(H[Q])$, Aut(G) has blocks of size p - a contradiction.

This completes the proof of the lemma. □

To complete the proof of Theorem 2.1.7 for Aut(G) having blocks of size 2 and no block of size p, we may now assume that $\overline{\text{Aut}(G)}$ is not doubly transitive. As before, $e(G) \in \{1, 2\}$. By Theorem 1.0.6, we may identify $V(\overline{G})$ with Z_p so that

$$\{\overline{x+b} : b \in Z_p\} \subseteq \overline{\text{Aut}(G)} \subset \{\overline{ax+b} : a \in Z_p^*, b \in Z_p\}. \tag{2.1}$$

One important consequence of (2.1) that we shall use frequently is that a member of $\overline{\text{Aut}(G)}$ that fixes two distinct vertices in $V(\overline{G})$ must be the identity. Since by (2.1), the mapping $\overline{x} \mapsto \overline{x+1}$ is in $\overline{\text{Aut}(G)}$, we may assume that the automorphism τ of G acts as previously defined, that is, for all $i \in Z_p$, $\tau(i) = i+1$ and $\tau(i') = (i+1)'$. The next lemma shows that no vertex of G is joined to two vertices in the same block.

Lemma 2.2.5 *If i and j are in Z_p, then at least one of ij and ij' is not in $E(G)$ and at least one of $i'j$ and $i'j'$ is not in $E(G)$.*

PROOF. Since $\tau \in$ Aut(G), it suffices to show that if $a \in Z_p^*$, then $0a$ and $0a'$ cannot both be in $E(G)$. Assume the contrary. Then, by applying τ^a to $0a$ and $0a'$, we get that both $a(2a)$ and $a(2a)'$ are edges. Moreover, since $e(G) \leq 2$, neither $a'(2a)$ nor $a'(2a)'$ is in $E(G)$. Also, neither $0'a$ nor $0'a'$ is in $E(G)$. Now G has an automorphism θ that maps $\{0, a\}$ to $\{0, a'\}$. Hence either

(*1*) $\theta(0) = 0$ and $\theta(a) = a'$, or

(2) $\theta(0) = a'$ and $\theta(a) = 0$.

In the first case, $\overline{\theta}$ fixes both $\overline{0}$ and $\overline{a}$ and hence is the identity. Thus $\overline{\theta}$ fixes $\overline{2a}$. Since $\theta(a) = a'$, $\theta(a') = a$ and so $\theta(\{a, 2a, (2a)'\}) = \{a', 2a, (2a)'\}$. However, $G[\{a', 2a, (2a)'\}]$ is an edgeless graph, while $G[\{a, 2a, (2a)'\}]$ is not - a contradiction.

In the second case, $\theta(0') = a$ and $\theta(a') = 0'$. Thus $\theta(\{0, a'\}) = \{0', a'\}$. Since $0a' \in E(G)$, we should have $0'a' \in E(G)$ - a contradiction. □

On combining the last lemma with the following result we get that no vertex of G is joined to vertices in both A and A', where we recall that $A = \{0, 1, \ldots, p-1\}$ and $A' = \{0', 1', \ldots, (p-1)'\}$.

Lemma 2.2.6 *If i, j, and k are distinct elements of Z_p, then at least one of ki and kj' is not in $E(G)$, and at least one of $k'i$ and $k'j'$ is not in $E(G)$.*

PROOF. It suffices to prove the first assertion. Assume that Z_p does contain distinct elements i, j, and k such that both ki and kj' are in $E(G)$. As the automorphism τ^{-k} maps k to 0, we lose no generality in assuming that $k = 0$. Then, as G is edge-transitive, there is an automorphism θ of G such that $\theta(\{0, i\}) = \{0, j'\}$. Hence either

(1) $\theta(0) = 0$ and $\theta(i) = j'$, or

(2) $\theta(0) = j'$ and $\theta(i) = 0$.

Consider the first case. As $\overline{\mathrm{Aut}(G)} \subset \{\overline{ax + b} : a \in Z_p^*, b \in Z_p\}$, there exist $a \in Z_p^*$ and $b \in Z_p$ such that $\overline{\theta}(\overline{x}) = \overline{ax + b}$ for all $x \in Z_p$. Now $\overline{\theta}(\overline{0}) = \overline{0}$ and $\overline{\theta}(\overline{i}) = \overline{j}$, so $\overline{\theta}(\overline{x}) = \overline{ji^{-1}x}$ for all $x \in Z_p$. In particular, $\overline{\theta}(\overline{ti}) = \overline{tj}$ for all t in Z. Thus $\theta(ti) \in \{tj, (tj)'\}$ and we show next that, for all non-negative integers t,

$$\theta(ti) = \begin{cases} tj & \text{if } t \text{ is even} \\ (tj)' & \text{if } t \text{ is odd.} \end{cases} \tag{2.2}$$

We prove (2.2) by induction. It is certainly true if t is 0 or 1. Suppose that (2.2) holds for all integers not exceeding t. We also assume initially that t is odd. We want to prove that, in that case, $\theta((t+1)i) = (t+1)j$. If not, then $\theta((t+1)i) = ((t+1)j)'$ and so

$$\tau^{-tj}\theta\tau^{ti}(\{0,i\}) = \tau^{-tj}\theta(\{ti,(t+1)i\}) = \tau^{-tj}(\{(tj)',((t+1)j)'\}) = \{0',j'\}.$$

Since $0i \in E(G)$, $0'j' \in E(G)$. But $0j'$ is also in $E(G)$, and we have a contradiction to the previous lemma.

If t is even and if $\theta((t+1)i) = (t+1)j$, then

$$\tau^{-tj}\theta\tau^{ti}(\{0,i\}) = \tau^{-tj}\theta(\{ti,(t+1)i\}) = \tau^{-tj}(\{tj,(t+1)j\}) = \{0,j\}.$$

Since $0i \in E(G)$, we must have $0j \in E(G)$. But we also have $0j' \in E(G)$, contradicting Lemma 2.2.5. Hence, if t is even, $\theta((t+1)i) = ((t+1)j)'$, and by induction, (2.2) holds. Thus, as p is odd, $\theta(pi) = (pj)'$, that is, $\theta(0) = 0'$ - a contradiction.

In the second case, we let $\sigma = \tau^{-j}\theta$. Then $\sigma(0) = 0'$ and $\sigma(i) = -j$. Thus $\overline{\sigma}(\overline{0}) = \overline{0}$ and $\overline{\sigma}(\overline{i}) = \overline{-j}$ so that, by (2.1), we have $\overline{\sigma}(\overline{x}) = \overline{-ji^{-1}x}$. Hence $\overline{\sigma}(\overline{ti}) = \overline{-tj}$ for all t in Z. Thus $\sigma(ti) \in \{-tj, (-tj)'\}$, and we show that, for all non-negative integers t,

$$\sigma(ti) = \begin{cases} (-tj)' & \text{if } t \text{ is even} \\ -tj & \text{if } t \text{ is odd.} \end{cases} \tag{2.3}$$

This statement is true for $t = 0$ and $t = 1$. Suppose (2.3) holds for all positive integers not exceeding t. If t is odd and $\sigma((t+1)i) = -(t+1)j$, then

$$\tau^{(t+1)j}\sigma\tau^{ti}(\{0,i\}) = \tau^{(t+1)j}\sigma(\{ti,(t+1)i\}) = \tau^{(t+1)j}(\{-tj,-(t+1)j\}) = \{j,0\}$$

so that $0j \in E(G)$. But, by Lemma 2.2.5, this contradicts the assumption that $0j' \in E(G)$. Hence $\sigma((t+1)i) = (-(t+1)j)'$.

If t is even and if $\sigma((t+1)i) = (-(t+1)j)'$, then

$$\tau^{(t+1)j}\sigma\tau^{ti}(\{0,i\}) = \tau^{(t+1)j}\sigma(\{ti,(t+1)i\}) = \tau^{(t+1)j}(\{(-tj)',(-(t+1)j)'\}) = \{j',0'\}$$

so that $0'j' \in E(G)$, contradicting $0j' \in E(G)$. Hence $\sigma((t+1)i) = -(t+1)j$ if t is even.

Therefore, by induction, (2.3) holds. But then, as in the first case, $\sigma(0) = \sigma(pi) = -pj = 0$, a contradiction.

This completes the proof. $\square$

We now establish that every edge of G must join a vertex in A to a vertex in A'.

Lemma 2.2.7 *Both $G[A]$ and $G[A']$ are edgeless graphs.*

PROOF. Suppose that $ij \in E(G)$ for some $i, j \in Z_p$, $i \neq j$. Then $\tau^{-i}(ij) \in E(G)$, that is, $0(j-i) \in E(G)$. If $0k' \in E(G)$ for some $k \in Z_p$, then we have a contradiction by one of the Lemmas 2.2.5 and 2.2.6. Hence $N(0) \subseteq A$, and so, for all $m \in Z_p$,

$$N(m) = N(\tau^m(0)) = \tau^m(N(0)) \subseteq A.$$

Thus G has no edge joining A and A'. But then, for all i, A_i is not a block of $\mathrm{Aut}(G)$ - a contradiction.

Hence $G[A]$ is an edgeless graph and, by symmetry, so is $G[A']$. $\square$

Now, by Lemma 2.2.7, G is bipartite with A and A' as its vertex classes. But then A and A' are blocks of $\mathrm{Aut}(G)$, contradicting the assumption that $\mathrm{Aut}(G)$ has no blocks of size p.

This completes the proof of Theorem 2.1.7.

Chapter 3

Half-transitive graphs

3.1 Bouwer's family of $\frac{1}{2}$-transitive graphs

In [16], where he proved that every vertex- and edge-transitive graph of odd degree is arc-transitive (see Proposition 2.1.2), Tutte stated that it was not known whether this extends to vertex- and edge-transitive graphs of even degree. This question was first answered in the negative by Bouwer [5]. In fact, Bouwer was able to prove the following.

Theorem 3.1.1 *For each integer $N \geq 2$, there exists a $\frac{1}{2}$-transitive graph of degree $2N$.*

We present Bouwer's proof of Theorem 3.1.1 in this section.

He starts by constructing a wider class of graphs. Let N, m, and n be integers greater than 1 such that

$$2^m \equiv 1 \pmod{n}. \tag{3.1}$$

Let the graph $X(N, m, n)$ have the vertex set $V = Z_m \times (Z_n)^{N-1}$ and let the vertices $\alpha = (i, a_2, a_3, \ldots, a_N)$ and $\beta = (i+1, b_2, b_3, \ldots, b_N)$ be adjacent whenever either

(*1*) $b_r = a_r$ for $r = 2, 3, \ldots, N$, or

(*2*) there exists a unique $k \in \{2, 3, \ldots, N\}$ such that $b_k \neq a_k$; for this k, $b_k = a_k + 2^i$.

(Note that the operations are always carried out in the appropriate ring, that is, either Z_m or Z_n.) The edge $\alpha\beta$ is called of *type* k, if (2) holds; otherwise, $\alpha\beta$ is of *type* 1. Since $a_k + 2^i = a_k$ for $i \in Z_m$ would imply $2^m \equiv 0 \pmod{n}$, contradicting (3.1), the types of the edges are well-defined. We note that for $m \geq 3$, the graph $X(N, m, n)$ is regular of degree $2N$, each vertex being incident with exactly two edges of each of the N types.

Proposition 3.1.2 *The graph $X(N, m, n)$ is vertex- and edge-transitive.*

PROOF. Denoting, generically, a vertex and its image (with respect to a mapping from V to V) by $(i, a_2, \ldots, a_N)$ and $(i', a'_2, \ldots, a'_N)$, respectively, we define mappings S_k, R, and T_k ($k = 2, 3, \ldots, N$) from V to V as follows:

$$\begin{array}{lll} S_k: & i' = i; & a'_k = a_k + 1 \text{ and } a'_r = a_r \text{ for } r \neq k; \\ R: & i' = i - 1; & a'_r = 1 + 2^{-1}a_r \text{ for all } r \in \{2, 3, \ldots, N\}\ ; \\ T_k: & i' = i; & a'_k = 2^i - \sum_{s=2}^{N} a_s \text{ and } a'_r = a_r \text{ for } r \neq k. \end{array}$$

Notice that, by (3.1), the element 2^{-1} is defined in Z_n. It is easy to see that these mappings are bijections. To see that they are automorphisms, let $\alpha = (i, a_2, \ldots, a_N)$ and $\beta = (i+1, b_2, \ldots, b_N)$ be adjacent vertices, and let, for $\theta \in \{S_k : k = 2, \ldots, N\} \cup \{R\} \cup \{T_k : k = 2, \ldots, N\}$, $\theta((i, a_2, \ldots, a_N)) = (i', a'_2, \ldots, a'_N)$ and $\theta((i+1, b_2, \ldots, b_N)) = (i'+1, b'_2, \ldots, b'_N)$. We observe the following. If $\theta = S_k$, then $i' = i$ and $b'_r - a'_r = b_r - a_r$ for all $r \in \{2, \ldots, N\}$. If $\theta = R$, then $i' = i - 1$ and $b'_r - a'_r = 2^{-1}(b_r - a_r)$ for all $r \in \{2, \ldots, N\}$. If $\theta = T_k$, then $i' = i$, $b'_r - a'_r = b_r - a_r$ for $r \neq k$, and

$$b'_k - a'_k = (2^{i+1} - \sum_{s=2}^{N} b_s) - (2^i - \sum_{s=2}^{N} a_s) = 2^i - \sum_{s=2}^{N}(b_s - a_s) = \begin{cases} 2^i & \text{if } \alpha\beta \text{ is of type 1} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, S_k, R, and T_k ($k = 2, \ldots, N$) are automorphisms of the graph.

To show that $X(N, m, n)$ is vertex-transitive, take any vertex $\alpha = (i, a_2, \ldots, a_N) \in V$ and let $\beta = R^i(\alpha)$. Then β is of the form $(0, b_2, \ldots, b_N)$. Now, under S_k ($k =$

$2, 3, \ldots, N)$, the k-th coordinate of a vertex increases by 1 (modulo n) while the other coordinates remain unchanged. It follows that $S_2^{-b_2} S_3^{-b_3} \ldots S_N^{-b_N}(0, b_2, \ldots, b_N) = (0, 0, \ldots, 0)$. Since $\alpha \in V$ was arbitrary, we deduce that the graph is vertex-transitive.

Let $\alpha = (2, 2, 2, \ldots, 2)$ and $\beta = (3, 2, 2, \ldots, 2)$ be vertices in the graph. Then

$$R(\beta) = \alpha \text{ and } R(\alpha) = (1, 2, 2, \ldots, 2);$$

$$S_k^{2N-4} T_k(\alpha) = \alpha \text{ and } S_k^{2N-4} T_k(\beta) = (3, c_2, c_3, \ldots, c_N),$$

where $c_k = 6$ and $c_r = 2$ for $r \neq k$; and

$$S_k^{2N-4} T_k R(\beta) = \alpha \text{ and } S_k^{2N-4} T_k R(\alpha) = (1, d_2, d_3, \ldots, d_N),$$

where $d_k = 0$ and $d_r = 2$ for $r \neq k$. Hence the mappings R, $S_k^{2N-4} T_k$, and $S_k^{2N-4} T_k R$ transform the edge $\alpha\beta$ to each of the other edges incident with α. We conclude that, since the graph is vertex-transitive, it is edge-transitive. □

Bouwer mentions in his paper [5] that for some triples (N, m, n) (e.g. $(2, 3, 7)$, $(2, 6, 7)$, and $(2, 4, 5)$) the graphs $X(N, m, n)$ are also arc-transitive. However, he then shows that the graphs $X(N, 6, 9)$, which we shall denote by X_N, are not arc-transitive. This is done by classifying the 6-cycles in the graph and showing that if X_N is arc-transitive, there must be an automorphism which maps a 6-cycle onto a 6-cycle of a type that does not appear in the graph.

Let C be a t-cycle in X_N. If C can be traversed in such a way that the first coordinates of the vertices in C occur in the sequence $i_1, i_2, \ldots, i_t$, then $\langle\langle i_1, i_2, \ldots, i_t \rangle\rangle$ will be called a *traversing sequence* of C. Traversing sequences of the same cycle are called *equivalent.*

It is easy to see that the only possible non-equivalent traversing sequences of a 4-cycle in X_N are

(q_1) $\langle\langle i, i+1, i+2, i+1 \rangle\rangle$ and

(q_2) $\langle\langle i, i+1, i, i+1 \rangle\rangle$.

Similarly, the only possible non-equivalent traversing sequences of a 6-cycle in X_N are

(h_1) $\langle\langle i, i+1, i+2, i+3, i+4, i+5\rangle\rangle$,

(h_2) $\langle\langle i, i+1, i, i+1, i, i+1\rangle\rangle$,

(h_3) $\langle\langle i, i+1, i+2, i+1, i, i+1\rangle\rangle$,

(h_4) $\langle\langle i, i+1, i+2, i+1, i+2, i+1\rangle\rangle$, and

(h_5) $\langle\langle i, i+1, i+2, i+3, i+2, i+1\rangle\rangle$.

This information will be used in the following lemma.

Lemma 3.1.3 *The graph $X_N = X(N,6,9)$ has girth 6. Any 6-cycle C in the graph has a traversing sequence (h_1), (h_2), or (h_3). The following can be said about the types of the edges in C with respect to its traversing sequence.*

(h_1) Each pair of opposite edges are of the same type.

(h_2) Each pair of opposite edges are of the same type with different pairs being of different types.

(h_3) The edges alternate between two distinct types.

Moreover, all of those possibilities are in fact realized in the graph.

PROOF. By construction, X_N contains no loops or multiple edges. Also, since $m = 6$ is even, X_N contains no odd cycle so that it is bipartite. Hence X_N has girth at least 4. We shall explore the cycles of length 4 and 6 in X_N.

Let C be a fixed t-cycle for $t \in \{4,6\}$. For any $k \in \{2,3,\ldots,N\}$ and any edge e of C define

$$c(k,e) = \begin{cases} 1 & \text{if } e \text{ is of type } k \\ 0 & \text{otherwise.} \end{cases}$$

We observe the following simple facts.

(a) Since the edge types are well-defined, for any edge e of C, $c(k,e) = 1$ for at most one $k \in \{2,3,\ldots,N\}$.

(b) If the 2-path $\alpha\beta\gamma$ lies on C and if the first coordinates of α and γ are equal, then the edges $\alpha\beta$ and $\beta\gamma$ are of different types.

The edges of C will be denoted by $e_1, e_2, \ldots, e_t$ according to the traversal of C in which the first coordinates of the vertices encountered occur in the same order as in the given traversing sequence.

Let $k \in \{2, 3, \ldots, N\}$ and let $e = \alpha\beta$ be an edge on C. If $\alpha = (i, a_2, \ldots, a_N)$ and $\beta = (j, b_2, \ldots, b_N)$, then a_k and b_k are related by

$$b_k = a_k + c(k,e)2^i \quad \text{if } j = i+1,$$

and by

$$b_k = a_k - c(k,e)2^{i-1} \quad \text{if } j = i-1.$$

We call the term $c(k,e)2^i$, or respectively, $-c(k,e)2^{i-1}$, the *change* in the k-th coordinate as we pass from the vertex α to the vertex β along the edge e. In a traversal of C, where we start and end at the same vertex, the changes in the k-th coordinates of the successive vertices encountered must sum to zero. Thus we associate with C a linear equation (in Z_9) in the t variables $c(k, e_i)$, $i = 1, 2, \ldots, t$, with coefficients independent of k. From its solution, and the conditions (a) and (b), we readily determine the possible combinations of the edge types along C.

We now try to solve the linear equations associated with possible 4- and 6-cycles in X_N. We categorize these cycles according to their traversing sequences.

Case (q_1): traversing sequence $\langle\langle i, i+1, i+2, i+1 \rangle\rangle$. The equation corresponding to a 4-cycle with this traversing sequence is

$$c(k,e_1)2^i + c(k,e_2)2^{i+1} - c(k,e_3)2^{i+1} - c(k,e_4)2^i \equiv 0 \pmod 9$$

and, dividing both sides by 2^i and using the fact that we are looking for solutions in $\{0,1\}$, it can be reduced to

$$c(k,e_1) + 2c(k,e_2) = 2c(k,e_3) + c(k,e_4). \tag{3.2}$$

By observation (b), the edges e_1 and e_4 are of different types so that at least one of e_1 and e_4 is of type k', for some $k' \in \{2, \ldots, N\}$. Let $c(k', e_1) = \delta$ and $c(k', e_4) = 1 - \delta$ where $\delta \in \{0, 1\}$. The equation (3.2) is then of the form $1 + 2x = 2y$ and thus has no solution in $\{0, 1\}$.

Case (q_2): traversing sequence $\langle\langle i, i+1, i, i+1\rangle\rangle$. We similarly obtain the equation

$$c(k, e_1) + c(k, e_3) = c(k, e_2) + c(k, e_4). \tag{3.3}$$

Since by (b), any two consecutive edges must be of different types, there exists $k' \in \{2, \ldots, N\}$ such that $c(k', e_1) = \delta$ and $c(k', e_2) = 1 - \delta$ for some $\delta \in \{0, 1\}$. The equation (3.3) is then simplified to $1 + x = 0$ which has no solution in $\{0, 1\}$.

We conclude that X_N has no 4-cycle.

Case (h_1): traversing sequence $\langle\langle i, i+1, i+2, i+3, i+4, i+5\rangle\rangle$. After simplifying the equation using the fact that $2^3 \equiv -1 \pmod 9$ and rearranging the terms we obtain

$$c(k, e_1) + 2c(k, e_2) + 4c(k, e_3) = c(k, e_4) + 2c(k, e_5) + 4c(k, e_6). \tag{3.4}$$

One possibility is that all edges are of type 1. If not, then, without loss of generality, we may assume that e_1 is of type $k' \in \{2, \ldots, N\}$, that is, $c(k', e_1) = 1$. Using $k = k'$ in (3.4) we can see that we must have $c(k', e_4) = 1$ since otherwise one side of the equation is odd while the other side is even. Similarly we can check that each of the other two pairs of opposite edges are of the same type.

Case (h_2): traversing sequence $\langle\langle i, i+1, i, i+1, i, i+1\rangle\rangle$. The equation can be reduced to

$$c(k, e_1) + c(k, e_3) + c(k, e_5) = c(k, e_2) + c(k, e_4) + c(k, e_6). \tag{3.5}$$

By (b), no two consecutive edges are of the same type. Fix $j \in \{1, 2, \ldots, 6\}$. If e_j is of type k' for some $k' \in \{2, \ldots, N\}$, then $c(k', e_j) = 1$ and $c(k', e_{j-1}) = c(k', e_{j+1}) = 0$. The equation (3.5) for $k = k'$ then implies $c(k', e_{j+2}) = c(k', e_{j+4}) = 0$ and $c(k', e_{j+3}) = 1$. From this it follows that each pair of opposite edges are of the same type and that different pairs are of different types.

Case (h_3): traversing sequence $\langle\langle i, i+1, i+2, i+1, i, i+1\rangle\rangle$. We simplify the equation to

$$c(k, e_1) + 2c(k, e_2) + c(k, e_5) = 2c(k, e_3) + c(k, e_4) + c(k, e_6). \tag{3.6}$$

By (b), e_2 and e_3 are of different types, e_4 and e_5 are of different types, and so are e_6 and e_1. Hence there exist $k' \in \{2, \ldots, N\}$ and $\delta \in \{0, 1\}$ such that $c(k', e_2) = \delta$ and $c(k', e_3) = 1 - \delta$. Using $k = k'$ in (3.6) we then have

$$4\delta + c(k', e_1) + c(k', e_5) = 2 + c(k', e_4) + c(k', e_6)$$

with the only solution $c(k', e_4) = c(k', e_6) = \delta$ and $c(k', e_1) = c(k', e_5) = 1 - \delta$. Thus there are three alternate edges of C that are of the same type $k' \in \{2, \ldots, N\}$. By (b) none of the remaining edges can be of the type k' so that if they are not all of type 1, then one of them is of type $k'' \neq k'$, $k'' \in \{2, \ldots, N\}$. Setting $k = k''$ in (3.6) we find, similarly as above, that all three of the remaining edges are of the same type $k'' \neq k'$.

Case (h_4): traversing sequence $\langle\langle i, i+1, i+2, i+1, i+2, i+1 \rangle\rangle$. We obtain the equation

$$c(k, e_1) + 2c(k, e_2) + 2c(k, e_4) = 2c(k, e_3) + 2c(k, e_5) + c(k, e_6). \tag{3.7}$$

By (b), e_1 and e_6 are of different types. Hence there exist $k' \in \{2, \ldots, N\}$ and $\delta \in \{0, 1\}$ such that $c(k', e_1) = \delta$ and $c(k', e_6) = 1 - \delta$. Now, setting $k = k'$ in equation (3.7), one side of the equation is odd while the other side is even, a contradiction.

Case (h_5): traversing sequence $\langle\langle i, i+1, i+2, i+3, i+2, i+1 \rangle\rangle$. The equation is

$$c(k, e_1) + 2c(k, e_2) + 4c(k, e_3) = 4c(k, e_4) + 2c(k, e_5) + c(k, e_6) \tag{3.8}$$

and since e_1 and e_6 must be of different types, the same argument as in Case (h_4) yields a contradiction.

From the solutions we found in cases (h_1), (h_2), and (h_3) it follows that all possibilities listed in the statement of the lemma are realized in the graph. □

If $e_1, e_2, \ldots, e_s$ are edges of the graph X_N, let $X_N[e_1, e_2, \ldots, e_s]$ denote the subgraph of X_N induced by the edge set $\{e_1, e_2, \ldots, e_s\}$. Adjacent edges e and f of the graph X_N will be called *opposed* if the three vertices of $X_N[e, f]$ have pairwise distinct first coordinates, and *properly opposed* if they are opposed and of different type.

Lemma 3.1.4 *Let e and f be two adjacent edges of the graph X_N. If e and f are properly opposed, the subgraph $X_N[e, f]$ is contained in exactly $N + 1$ distinct 6-cycles. Otherwise, $X_N[e, f]$ is contained in exactly N distinct 6-cycles. In each case, the 6-cycles are pairwise disjoint except for the three vertices and the two edges of $X_N[e, f]$.*

PROOF. Let $e = \alpha\beta$ and $f = \beta\gamma$.

If e and f are properly opposed, we may assume that the first coordinates of the vertices α, β, and γ are, respectively, j, $j + 1$, and $j + 2$, that e is of type k' and that f is of type $k'' \neq k'$. Let C be a 6-cycle that contains $X_N[e, f]$. Then, by Lemma 3.1.3, the traversing sequence of C is either (h_1) or (h_3). In case (h_1), C is uniquely defined by choosing the type k''' for the third pair of opposite edges. Hence there are N possibilities. In case (h_3), C is uniquely defined by e and f. Thus a pair of properly opposed edges lie in exactly $N + 1$ 6-cycles.

Now let e and f be opposed but not properly opposed. Then e and f are of the same type k' and, again, we may assume that the first coordinates of the vertices α, β, and γ are j, $j+1$, and $j+2$, respectively. If C is a 6-cycle that contains $X_N[e, f]$, then C must fall under case (h_1) of Lemma 3.1.3 and thus is uniquely defined by the choice of the type of the third pair of opposite edges. This produces exactly N possibilities.

Finally, suppose that e and f are not opposed. Then, by (b), they must be of different types, and the first coordinates of the vertices α, β, and γ are either

(*1*) j, $j + 1$, and j, or

(*2*) $j + 1$, j, and $j + 1$,

respectively. In either case, if C is a 6-cycle that contains $X_N[e, f]$, then the traversing sequence of C is either (h_2) or (h_3). With traversing sequence (h_2), C is uniquely defined by the choice of the type of the third pair of opposite edges. Since this type must be distinct from the types of e and f, we have $N - 2$ possibilities. With traversing sequence (h_3), there are two possibilities. In case (1), either $e = e_2$ and $f = e_3$ or $e = e_5$ and $f = e_6$. In case (2), either $e = e_4$ and $f = e_5$ or $e = e_6$ and $f = e_1$. Thus in both cases there are altogether N 6-cycles containing $X_N[e, f]$.

Now suppose that $C = \alpha\beta\gamma\delta\varepsilon\phi$ and $C' = \alpha\beta\gamma\delta'\varepsilon'\phi'$ are distinct 6-cycles containing the edges $e = \alpha\beta$ and $f = \beta\gamma$. Since, checking the possibilities listed in Lemma 3.1.3, any three consecutive edges lie in at most one 6-cycle, $\delta \neq \delta'$ and $\phi \neq \phi'$. Suppose that $\varepsilon = \varepsilon'$. Then $\gamma\delta\varepsilon\delta'$ is a 4-cycle, contradicting Lemma 3.1.3. Hence C and C' are disjoint except for the edges e and f. □

Corollary 3.1.5 *Properly opposed edges remain properly opposed under any automorphism of the graph.*

PROOF. An automorphism of the graph preserves the number of 6-cycles in which a pair of adjacent edges lie. The result then follows by Lemma 3.1.4. □

We now present Bouwer's proof of the main result.

Proposition 3.1.6 *The graphs $X_N = X(N, 6, 9)$ are not arc-transitive.*

PROOF. We treat the cases $N \geq 3$ and $N = 2$ separately.

Case $N \geq 3$. Let $e = \alpha\beta$ be any given edge of the graph, $\alpha = (i, a_2, \ldots, a_N)$, $\beta = (i + 1, b_2, \ldots, b_N)$. Since $N \geq 3$, there exist two distinct edges $d_1 = \alpha\delta_1$ and $d_2 = \alpha\delta_2$ which are properly opposed to e. The edges e, d_1, and d_2 are of distinct types. Let the type of d_i be k_i $(i = 1, 2)$. Let c_i be the edge of type k_{3-i} properly opposed to d_i, having the vertex δ_i in common with d_i $(i = 1, 2)$. Now, if X_N is arc-transitive, then there exists an automorphism θ which interchanges the vertices α and β. By Corollary 3.1.5, θ maps the subgraph $X_N[c_1, d_1, d_2, c_2]$ to a subgraph $X_N[c_1', d_1', d_2', c_2']$, where $d_1' = \beta\delta_1'$ and $d_2' = \beta\delta_2'$ are edges properly opposed to e while $c_i' = \delta_i'\gamma_i'$ $(i = 1, 2)$ is an edge properly opposed to d_i' (see Figure 3.1). However, the subgraph $X_N[c_1, d_1, d_2, c_2]$ is seen to be contained in a 6-cycle (with traversing sequence (h_3)), while considering the first coordinates of its vertices, we deduce from

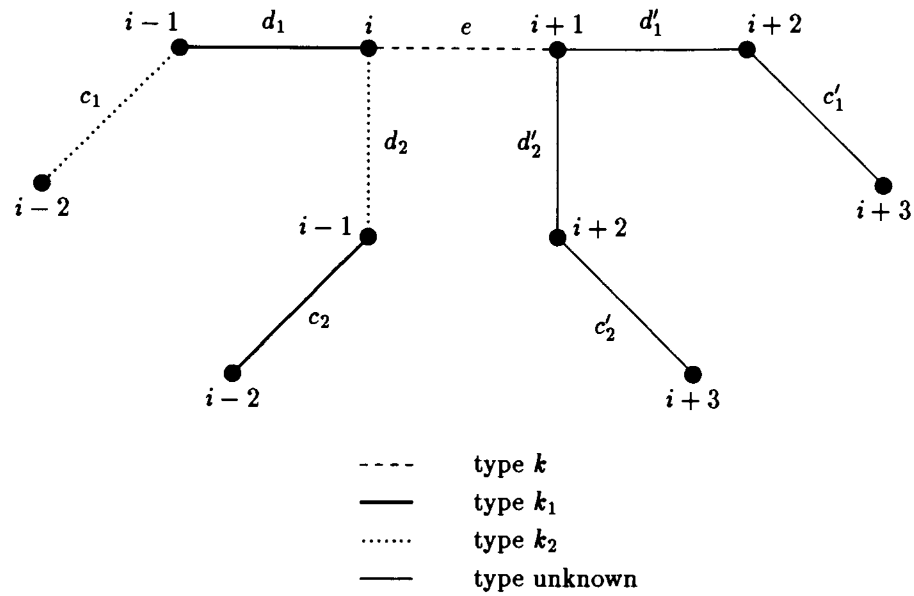

Figure 3.1: Proposition 3.1.6, Case $N \geq 3$

Lemma 3.1.3 that the subgraph $X_N[c_1', d_1', d_2', c_2']$ is not contained in a 6-cycle. This is a contradiction.

Case $N = 2$. In this case, there are only two possible types for an edge. Consequently, it is not difficult to see that for any given edge e, there is a unique cycle C that contains e such that any two adjacent edges in C are properly opposed. By tracing out C, we find it to be an 18-cycle. Let $e = \alpha\beta$, $\alpha = (i, a_2)$ and $\beta = (i+1, b_2)$. Let $e_1 = \beta\beta_1$ and $f_1 = \alpha\alpha_1$ be edges properly opposed to e. Define inductively, for $i = 2, 3, 4, 5$, the edges $e_i = \beta_{i-1}\beta_i$ and $f_i = \alpha_{i-1}\alpha_i$ to be properly opposed to e_{i-1} and f_{i-1}, respectively. As mentioned above, these edges lie on an 18-cycle so that they are pairwise distinct. The subgraph $X_N[e_1, e_2, e_3]$ has vertices β, β_1, β_2, and β_3 whose first coordinates are $i+1$, $i+2$, $i+3$, and $i+4$, respectively. Checking the possibilities in Lemma 3.1.3 we can see that $X_N[\acute{e_1}, e_2, e_3]$ is contained in a unique 6-cycle C_1 (with traversing sequence (h_1)). The edges of C_1 are, in order, e_1, e_2, e_3, h_1, h_2, and h_3, where $h_1 \neq e_4$ since h_1 is of the same type as e_1 (by Lemma 3.1.3)

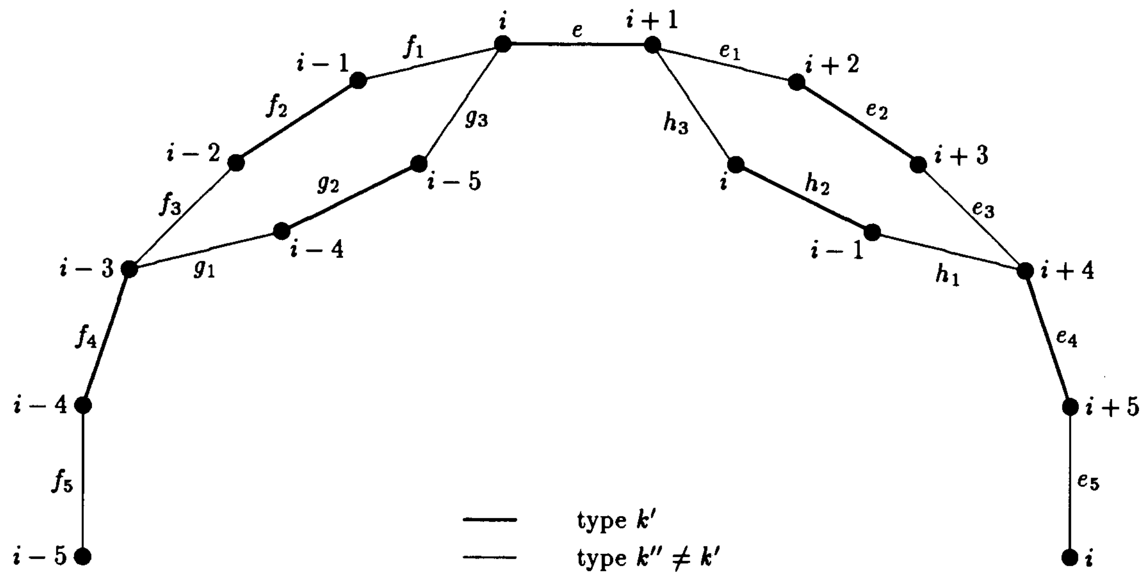

Figure 3.2: Proposition 3.1.6, Case $N = 2$

and e_4 is not. Also, $h_3 \neq e$ since h_3 is of the same type as e_3 and e is not. Similarly, $X_N[f_1, f_2, f_3]$ has vertices α, α_1, α_2, and α_3 whose first coordinates are, respectively, i, $i-1$, $i-2$, and $i-3$ so that $X_N[f_1, f_2, f_3]$ is contained in a unique 6-cycle C_2 (which has traversing sequence (h_1)). The edges of C_2 are, in order, f_1, f_2, f_3, g_1, g_2, and g_3, where $g_1 \neq f_4$ and $g_3 \neq e$ since g_1 and f_4, as well as g_3 and e, are of distinct types (see Figure 3.2).

Now, if X_N is arc-transitive, there exists an automorphism θ of X_N that interchanges the vertices α and β. Then θ must map the 18-cycle C to itself and thus interchange the 6-cycles C_1 and C_2. Consequently, θ interchanges the subgraphs $X_N[g_2, g_1, f_4, f_5]$ and $X_N[h_2, h_1, e_4, e_5]$. The first coordinates of the vertices in $X_N[g_2, g_1, f_4, f_5]$ are $i-5$, $i-4$, $i-3$, $i-4$, and $i-5$, respectively, and checking the types of these edges, we can see that $X_N[g_2, g_1, f_4, f_5]$ lies in a 6-cycle with traversing sequence (h_3). On the other hand, the first coordinates of the vertices in $X_N[h_2, h_1, e_4, e_5]$ are, in order, i, $i-1$, $i-2$, $i-1$, and i, so that $X_N[h_2, h_1, e_4, e_5]$

is not contained in a 6-cycle by Lemma 3.1.3. This is a contradiction.

We conclude that the graphs $X_N = X(N,6,9)$ are $\frac{1}{2}$-transitive. □

3.2 Metacirculant graphs $M(\alpha; m, n)$

In sections 3.2, 3.3, and 3.4 we talk about a large family of graphs which proves to be a rich source of $\frac{1}{2}$-transitive graphs. These graphs are called metacirculants and were first defined by Alspach and Parsons in [1]. In fact, we will only be interested in a subfamily of metacirculant graphs, namely, the graphs $M(\alpha; m, n)$, which are vertex- and edge-transitive. Among these graphs we find several infinite families of $\frac{1}{2}$-transitive graphs and, in particular, Holt's graph $M(4;3,9)$, which is the unique smallest $\frac{1}{2}$-transitive graph of degree 4. Furthermore, Xu has recently proved [17] that all $\frac{1}{2}$-transitive graphs of prime-cube order and degree 4 are metacirculants (see Theorem 3.3.4). This strengthens a conjecture of B. Alspach and D. Marušič which asserts that every $\frac{1}{2}$-transitive graph of degree 4 is a metacirculant. All this makes metacirculants extremely interesting in the context of $\frac{1}{2}$-transitivity, and yet, not much is known about them.

Most of this section follows Section 3 in [2]. Our Corollary 3.2.16, however, is a generalization of Corollary 3.8 in [2].

We first define general metacirculants as in [1]. Let

$$V = \{v_j^i : i \in Z_m, j \in Z_n\},$$

where superscripts and subscripts are always reduced modulo m and n, respectively. Let Z_n^* denote the multiplicative group of units of Z_n and let $\alpha \in Z_n^*$. We define two permutations ρ and τ on V by

$$\rho(v_j^i) = v_{j+1}^i \qquad \text{and} \qquad \tau(v_j^i) = v_{\alpha j}^{i+1}.$$

It is easy to see that $\langle \rho, \tau \rangle$ is a transitive permutation group on V. Notice that

$$\rho = (v_0^0\, v_1^0 \ldots v_{n-1}^0)(v_0^1\, v_1^1 \ldots v_{n-1}^1) \ldots\ldots (v_0^{m-1}\, v_1^{m-1} \ldots v_{n-1}^{m-1})$$

so that $\langle\rho\rangle$ is a cyclic group of order n with m orbits $V^0, V^1, \ldots, V^{m-1}$ where $V^i = \{v_j^i : j \in Z_n\}$ for $i = 0, 1, \ldots, m-1$.

Let a be the order of α in Z_n^*. We show that $b = \mathrm{lcm}(a, m)$ is the order of τ. We have

$$\tau^b(v_j^i) = v_{\alpha^b j}^{i+b} = v_j^i$$

since $b \equiv 0 \pmod{m}$ and $\alpha^b \equiv 1 \pmod{n}$. Hence $\tau^b = 1$ and the order of τ divides b. On the other hand, if $\tau^c = 1$, then

$$\tau^c(v_1^0) = v_1^0 = v_{\alpha^c}^c$$

so that $c \equiv 0 \pmod{m}$ and $\alpha^c \equiv 1 \pmod{n}$. Hence both m and a divide c and so b divides c. Thus the cyclic group $\langle\tau\rangle$ has order b.

Also, for any $v_j^i \in V$,

$$\tau\rho\tau^{-1}(v_j^i) = \tau\rho(v_{\alpha^{-1}j}^{i-1}) = \tau(v_{\alpha^{-1}j+1}^{i-1}) = v_{j+\alpha}^i = \rho^\alpha(v_j^i)$$

so that $\tau\rho\tau^{-1} = \rho^\alpha$. Thus the group $\langle\rho, \tau\rangle$ has the presentation

$$\langle \rho, \tau : \rho^n = 1 = \tau^b, \tau\rho\tau^{-1} = \rho^\alpha \rangle.$$

We would like to construct all graphs G with $V(G) = V$ such that $\langle\rho,\tau\rangle \leq \mathrm{Aut}(G)$. Let $\mu = \lfloor \frac{m}{2} \rfloor$. Notice that, if $\langle\rho,\tau\rangle \leq \mathrm{Aut}(G)$, then $v_j^i \sim v_{j+h}^{i+r}$ in G if and only if $\tau^{-i}(v_j^i) \sim \tau^{-i}(v_{j+h}^{i+r})$ if and only if $v_{\alpha^{-i}j}^0 \sim v_{\alpha^{-i}j+\alpha^{-i}h}^r$ if and only if $\rho^{-\alpha^{-i}j}(v_{\alpha^{-i}j}^0) \sim \rho^{-\alpha^{-i}j}(v_{\alpha^{-i}j+\alpha^{-i}h}^r)$ if and only if $v_0^0 \sim v_{\alpha^{-i}h}^r$. Hence, to construct such G it suffices to specify the sets

$$S_r = \{s \in Z_n : v_0^0 \sim v_s^r\}$$

for $0 \leq r \leq \mu$ and to determine what conditions these sets S_r must satisfy in order that $\langle\rho,\tau\rangle \leq \mathrm{Aut}(G)$.

Since we do not want G to have loops, $0 \notin S_0$ and since $\rho \in \mathrm{Aut}(G)$, we need $S_0 = -S_0$. Further, $s \in S_r$ if and only if $v_0^0 \sim v_s^r$ if and only if $\tau^m(v_0^0) \sim \tau^m(v_s^r)$ if and only if $v_0^0 \sim v_{\alpha^m s}^r$ if and only if $\alpha^m s \in S_r$. Thus $S_r = \alpha^m S_r$. If m is even, $s \in S_\mu$

if and only if $v_0^0 \sim v_s^\mu$ if and only if $\tau^\mu(v_0^0) \sim \tau^\mu(v_s^\mu)$ if and only if $v_0^\mu \sim v_{\alpha^\mu s}^0$ if and only if $\rho^{-\alpha^\mu s}(v_0^\mu) \sim \rho^{-\alpha^\mu s}(v_{\alpha^\mu s}^0)$ if and only if $v_{-\alpha^\mu s}^\mu \sim v_0^0$ if and only if $-\alpha^\mu s \in S_\mu$. Thus $S_\mu = -\alpha^\mu S_\mu$.

We summarize the above conditions as follows:

(1) $0 \notin S_0 = -S_0$,

(2) $\alpha^m S_r = S_r$ for $0 \leq r \leq \mu$,

(3) $\alpha^\mu S_\mu = -S_\mu$ if m is even,

(4) $E(G) = \{\{v_j^i, v_{j+h}^{i+r}\} : 0 \leq r \leq \mu \text{ and } h \in \alpha^i S_r\}$.

Definition 3.2.1 Let $m \geq 1$, $n \geq 2$, $\alpha \in Z_n^*$ and $\mu = \lfloor \frac{m}{2} \rfloor$. Also, let $S_0, S_1, \ldots, S_\mu$ be subsets of Z_n satisfying conditions (1) – (3). The *(m,n)-metacirculant* $G = G(m,n,\alpha,S_0,S_1,\ldots,S_\mu)$ is a graph with $V(G) = V$ and with $E(G)$ given by (4).

By the way we have obtained the definition of metacirculant graphs, the following result is immediate.

Theorem 3.2.2 *The metacirculant $G = G(m,n,\alpha,S_0,S_1,\ldots,S_\mu)$ is vertex-transitive with $\langle\rho,\tau\rangle \leq Aut(G)$. Conversely, any graph G' with vertex set V and $\langle\rho,\tau\rangle \leq Aut(G')$ is an (m,n)-metacirculant.*

We proceed to define the graphs $M(\alpha;m,n)$. Let $n \geq 5$ be an integer and let $\alpha \in Z_n^*$ be an element of order m or $2m$, where $m \geq 2$. Define $M(\alpha;m,n)$ to be the metacirculant $G(m,n,\alpha,\emptyset,\{-1,1\},\emptyset,\ldots,\emptyset)$. Notice that, if the order of α is $2m$, then $\alpha^m \equiv -1 \pmod n$ by condition (2) in the definition of a metacirculant. Thus $M(\alpha;m,n)$ is the graph with vertex set

$$V = \{v_j^i : i \in Z_m, j \in Z_n\}$$

and edge set

$$E = \{v_j^i v_{j+\delta\alpha^i}^{i+1} : i \in Z_m, j \in Z_n, \delta \in \{-1,1\}\}.$$

By Theorem 3.2.2, $M(\alpha;m,n)$ is vertex-transitive with $\langle\rho,\tau\rangle \leq \mathrm{Aut}(G)$. The orbits $V^0, V^1, \ldots, V^{m-1}$ of ρ will be referred to as the blocks of $M(\alpha;m,n)$ although they need not be blocks of imprimitivity of its automorphism group. Recall that, for general metacirculants, the order of τ is $\mathrm{lcm}(a, m)$ where a is the order of α. Hence for the graphs $M(\alpha; m, n)$, the order of τ is m. Also, for the mapping π defined by $\pi(v_j^i) = v_{-j}^i$, $\pi(v_j^i v_{j+\delta\alpha^i}^{i+1}) = v_{-j}^i v_{-j-\delta\alpha^i}^{i+1}$ so that π is another automorphism of $M(\alpha; m, n)$, which will prove useful. It is easy to check that $\pi\rho = \rho^{n-1}\pi$ and $\pi\tau = \tau\pi$. This, together with $\tau\rho = \rho^\alpha\tau$, implies

$$\langle \rho, \tau, \pi \rangle = \{\rho^i \tau^j \pi^k : 0 \leq i \leq n-1, 0 \leq j \leq m-1, 0 \leq k \leq 1\}.$$

We now establish the edge-transitivity of $M(\alpha; m, n)$.

Lemma 3.2.3 *$M(\alpha; m, n)$ is edge-transitive.*

PROOF. Let $e = v_j^i v_{j+\delta\alpha^i}^{i+1}$ (for some $\delta \in \{-1, 1\}$) be any edge of $M(\alpha; m, n)$. We have

$$\rho^{-\alpha^i j}\tau^{-i}(v_j^i v_{j+\delta\alpha^i}^{i+1}) = \rho^{-\alpha^i j}(v_{\alpha^{-i}j}^0 v_{\alpha^{-i}j+\delta}^1) = v_0^0 v_\delta^1.$$

Since also

$$\pi(v_0^0 v_{-1}^1) = v_0^0 v_1^1,$$

any edge can be mapped to $v_0^0 v_1^1$. Hence $M(\alpha; m, n)$ is edge-transitive. □

We shall see in Theorem 3.4.5 that the case $m = 2$ is not particularly interesting. Hence we assume for the rest of the section that $m \geq 3$. When testing the graphs $M(\alpha; m, n)$ for arc-transitivity, we will be dealing with a special kind of cycles, which we now define.

Definition 3.2.4 A cycle C of $M(\alpha; m, n)$ of length at least m is said to be *coiled* if every subpath of C having m vertices intersects each of $V^0, V^1, \ldots, V^{m-1}$.

It is easy to see that a coiled cycle must have length a multiple of m.

Definition 3.2.5 The *coiled girth* of $M(\alpha; m, n)$ is the length of a shortest coiled cycle in $M(\alpha; m, n)$.

Proposition 3.2.6 *The coiled girth of $M(\alpha; m, n)$ is either m or $2m$.*

PROOF. Assume that $M(\alpha; m, n)$ does not contain a coiled cycle of length m. Consider the closed trail

$$v_0^0\, v_1^1\, v_{1+\alpha}^2 \cdots v_{1+\alpha+\alpha^2+\ldots+\alpha^{m-2}}^{m-1}\, v_{1+\alpha+\alpha^2+\ldots+\alpha^{m-1}}^0\, v_{\alpha+\alpha^2+\ldots+\alpha^{m-1}}^1\, v_{\alpha^2+\ldots+\alpha^{m-1}}^2 \cdots v_{\alpha^{m-1}}^{m-1}\, v_0^0.$$

Since $M(\alpha; m, n)$ has no coiled cycles of length m, the vertices of the closed trail are pairwise distinct. Thus, it is a coiled cycle of length $2m$ and $M(\alpha; m, n)$ has coiled girth $2m$. $\square$

Using the coiled girth cycles of $M(\alpha; m, n)$ we obtain natural edge-partitions of $M(\alpha; m, n)$ as follows. If $M(\alpha; m, n)$ has coiled girth m, let C be a coiled m-cycle,

$$C = v_j^0\, v_{j+\delta_0}^1\, v_{j+\delta_0+\delta_1\alpha}^2 \cdots v_{j+\delta_0+\delta_1\alpha+\ldots+\delta_{m-2}\alpha^{m-2}}^{m-1}\, v_j^0,$$

where $\delta_i \in \{-1, 1\}$ for all $i \in \{0, \ldots, m-2\}$. Let $\rho(C)$ denote the coiled m-cycle obtained by applying ρ to the vertices of C, that is,

$$\rho(C) = v_{j+1}^0\, v_{j+1+\delta_0}^1\, v_{j+1+\delta_0+\delta_1\alpha}^2 \cdots v_{j+1+\delta_0+\delta_1\alpha+\ldots+\delta_{m-2}\alpha^{m-2}}^{m-1}\, v_{j+1}^0.$$

Then the coiled m-cycles $C, \rho(C), \rho^2(C), \ldots, \rho^{n-1}(C)$ are pairwise vertex-disjoint so that they form a 2-factor of $M(\alpha; m, n)$. It is not difficult to see that the remaining edges also form a 2-factor made up of coiled m-cycles $C', \rho(C'), \rho^2(C'), \ldots, \rho^{n-1}(C')$, where

$$C' = v_j^0\, v_{j-\delta_0}^1\, v_{j-\delta_0-\delta_1\alpha}^2 \cdots v_{j-\delta_0-\delta_1\alpha-\ldots-\delta_{m-2}\alpha^{m-2}}^{m-1}\, v_j^0.$$

We call the edge-partition $C, \rho(C), \rho^2(C), \ldots, \rho^{n-1}(C), C', \rho(C'), \rho^2(C'), \ldots, \rho^{n-1}(C')$ the *ρ-partition of $M(\alpha; m, n)$ induced by C.*

If the coiled girth of $M(\alpha; m, n)$ is $2m$, let C be a coiled $2m$-cycle with the property that of the two edges from V^i to V^{i+1} in C, one is of the form $v_{j_i}^i\, v_{j_i+\alpha^i}^{i+1}$ and the other is of the form $v_{j_i}^i\, v_{j_i-\alpha^i}^{i+1}$. (The proof of Proposition 3.2.6 gives an example of such a cycle.) Then the coiled $2m$-cycles $C, \rho(C), \rho^2(C), \ldots, \rho^{n-1}(C)$ are pairwise edge-disjoint so that they form a partition of the edge set of $M(\alpha; m, n)$ into $2m$-cycles. This partition is also called the *ρ-partition of $M(\alpha; m, n)$ induced by C.*

Definition 3.2.7 If $M(\alpha; m, n)$ has coiled girth m and the ρ-partition of $M(\alpha; m, n)$ induced by every coiled m-cycle yields the same 2-factorization of $M(\alpha; m, n)$, then we say that $M(\alpha; m, n)$ is *tightly coiled.* Otherwise, $M(\alpha; m, n)$ is *loosely coiled.* A similar definition applies in the case that the coiled girth of $M(\alpha; m, n)$ is $2m$. However, we show that in that case $M(\alpha; m, n)$ is always loosely coiled.

Lemma 3.2.8 *If $M(\alpha; m, n)$ has coiled girth $2m$, then it is loosely coiled.*

PROOF. We have seen in Proposition 3.2.6 that

$$C = v_0^0\, v_1^1\, v_{1+\alpha}^2 \cdots v_{1+\alpha+\alpha^2+\ldots+\alpha^{m-2}}^{m-1}\, v_{1+\alpha+\alpha^2+\ldots+\alpha^{m-1}}^{0}\, v_{\alpha+\alpha^2+\ldots+\alpha^{m-1}}^{1} \cdots v_{\alpha^{m-1}}^{m-1}\, v_0^0$$

is a coiled $2m$-cycle. Another coiled $2m$-cycle is

$$C' = v_0^0\, v_{-1}^1\, v_{-1+\alpha}^2 \cdots v_{-1+\alpha+\alpha^2+\ldots+\alpha^{m-2}}^{m-1}\, v_{-1+\alpha+\alpha^2+\ldots+\alpha^{m-1}}^{0}\, v_{\alpha+\alpha^2+\ldots+\alpha^{m-1}}^{1} \cdots v_{\alpha^{m-1}}^{m-1}\, v_0^0.$$

Clearly, C and C' induce distinct ρ-partitions. Hence $M(\alpha; m, n)$ is loosely coiled.

□

We now set about proving some lemmas which will be helpful in establishing that certain graphs $M(\alpha; m, n)$ are $\frac{1}{2}$-transitive.

Lemma 3.2.9 *Let $M = M(\alpha; m, n)$, $m \geq 3$. The subgraph $M[V^i, V^{i+1}]$ induced by the two adjacent blocks V^i and V^{i+1} is a $2n$-cycle if n is odd, and consists of two disjoint n-cycles if n is even.*

PROOF. Since $M[V^i, V^{i+1}]$ is 2-regular, it is a disjoint union of cycles. Now $v_j^i\, v_{j+\alpha^i}^{i+1}\, v_{j+2\alpha^i}^{i} \cdots v_{j+k\alpha^i}^{i+1}$ is a cycle in $M[V^i, V^{i+1}]$ if and only if k is the smallest positive even integer such that $k\alpha^i \equiv 0 \pmod{n}$. Since $\alpha \in Z_n^*$, $k\alpha^i \equiv 0 \pmod{n}$ if and only if $k \equiv 0 \pmod{n}$. Hence $k = 2n$ if n is odd, and $k = n$ if n is even. □

Lemma 3.2.10 *Let $M = M(\alpha; m, n)$, $m \geq 3$. If $\sigma \in \mathrm{Aut}(M)$ fixes two adjacent blocks pointwise, then σ is the identity.*

PROOF. Let σ fix V^i and V^{i+1} pointwise. Then σ fixes V^{i-1} setwise. By the previous lemma, $M[V^{i-1}, V^i]$ is either a $2n$-cycle or two n-cycles and σ fixes alternate vertices of the cycle(s). Hence σ fixes every vertex of the cycle(s) and thus it fixes V^{i-1} pointwise. Continuing in this way establishes the result. $\square$

Lemma 3.2.11 *Let* $M = M(\alpha; m, n)$, $m \geq 3$. *If* $\sigma \in \mathrm{Aut}(M)$ *fixes a block of* M *pointwise, then* σ *is the identity.*

PROOF. Without loss of generality we may assume that V^1 is the block of M fixed by σ. The neighbours of v_0^1 are v_1^0, v_{-1}^0, v_α^2, and $v_{-\alpha}^2$. The neighbours of v_2^1 are v_1^0, v_3^0, $v_{2+\alpha}^2$, and $v_{2-\alpha}^2$. Suppose that v_1^0 is not fixed by σ. Then v_0^1 and v_2^1 have another neighbour in common. Note that $v_{-1}^0 \neq v_3^0$ because $-1 \equiv 3 \pmod{n}$ contradicts $n \geq 5$. Clearly, $v_\alpha^2 \neq v_{2+\alpha}^2$ and $v_{-\alpha}^2 \neq v_{2-\alpha}^2$. Hence either $v_\alpha^2 = v_{2-\alpha}^2$ or $v_{-\alpha}^2 = v_{2+\alpha}^2$.

If $v_\alpha^2 = v_{2-\alpha}^2$, then $2\alpha \equiv 2 \pmod{n}$ so that, since $\alpha \neq 1$, $\alpha = \frac{n+2}{2}$. Hence n must be even. If n is a multiple of 4, say $n = 4k$, then $\alpha = 2k + 1$ so that $\alpha^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{n}$, contradicting $m \geq 3$. If $n = 4k + 2$ for some $k \in N$, then $\alpha = 2k + 2$, contradicting $\alpha \in Z_n^*$.

Similarly, if $v_{-\alpha}^2 = v_{2+\alpha}^2$, then $2\alpha \equiv -2 \pmod{n}$ so that, since $\alpha \neq -1$, $\alpha = \frac{n-2}{2}$. Again, n must be even. But $n = 4k$ implies $\alpha = 2k - 1$ so that $\alpha^2 \equiv 1 \pmod{n}$, and $n = 4k + 2$ implies $\alpha = 2k$, so that $\alpha \notin Z_n^*$. In both cases we have a contradiction.

Thus the only possibility is that σ fixes v_1^0. Continuing in this way we obtain that V^0 is fixed pointwise by σ. Hence by the preceding lemma σ is the identity.

$\square$

Lemma 3.2.12 *Let* $M = M(\alpha; m, n)$ *and suppose that whenever* $\sigma \in \mathrm{Aut}(M)$ *fixes two adjacent vertices of* M, σ *is the identity. Then either* $\mathrm{Aut}(M) = \langle \rho, \tau, \pi \rangle$ *or* $|\mathrm{Aut}(M)| = 2|\langle \rho, \tau, \pi \rangle|$.

PROOF. Let e be any edge of M. By hypothesis, if σ is an automorphism of M that fixes the edge e, then either σ is the identity or σ interchanges the endpoints of e and $\sigma^2 = 1$. Moreover, if σ_1 and σ_2 are two automorphisms that interchange the endpoints of e, then $\sigma_1\sigma_2 = 1$ so that $\sigma_2 = \sigma_1^{-1} = \sigma_1$. Hence the stabilizer of e either contains just the identity or it has order 2. Since M is edge-transitive, the Orbit-Stabilizer Theorem yields

$$|\mathrm{Aut}(M)| = |\mathrm{Aut}(M)_e| \cdot |E(M)| = |\mathrm{Aut}(M)_e| \cdot 2mn \in \{2mn, 4mn\}.$$

Since $|\langle \rho, \tau, \pi \rangle| = 2mn$, the result follows. □

Lemma 3.2.13 *Let m and n be odd, $m \geq 3$, and let $M = M(\alpha; m, n)$ have coiled girth m and be loosely coiled. Let $x \in V^i$ and let $y, y' \in V^{i-1}$ and $z, z' \in V^{i+1}$ be the four neighbours of x. Then each of the triples yxz, $y'xz$, yxz', and $y'xz'$ is contained in a coiled m-cycle.*

PROOF. Suppose that the triple yxz' is not contained in a coiled m-cycle. Then $y'xz$ is not contained in a coiled m-cycle either so that every coiled m-cycle through x contains either yxz or $y'xz'$. Since M is loosely coiled, there exist at least two coiled m-cycles C and C' that contain the triple yxz. Moreover, C and C' contain a triple uvw and uvw', respectively, such that $w' \neq w$. Let σ be an automorphism of M that takes v to x. Then $\sigma(C)$ and $\sigma(C')$ are m-cycles containing x. In fact, $\sigma(C)$ and $\sigma(C')$ are coiled because m is odd. But then either $\sigma(C)$ or $\sigma(C')$ is a coiled m-cycle that contains either yxz' or $y'xz$, contradicting the assumption. Hence the result follows. □

Lemma 3.2.14 *Let m and n be odd, $m \geq 3$, and let $M = M(\alpha; m, n)$ have coiled girth m and be loosely coiled. Then any automorphism of M that fixes two adjacent vertices is the identity.*

PROOF. Suppose $x \in V^i$ and $y \in V^{i-1}$ are two adjacent vertices of M fixed by $\sigma \in \mathrm{Aut}(M)$. Let y' be the other neighbour of x in V^{i-1} and let z and z' be the two neighbours of x in V^{i+1}. Then σ fixes $\{y', z, z'\}$ setwise. Since m is odd, M contains no non-coiled m-cycles. Hence the triple yxy' is not in an m-cycle. On the other hand, by Lemma 3.2.13, each of the two triples yxz and yxz' lies in an m-cycle. Therefore σ must also fix y' in addition to fixing x and y. For the same reason, σ must fix the other neighbour of y' in V^i. Since m is odd, $M[V^i, V^{i-1}]$ is a $2n$-cycle so that, continuing in this way, we see that σ fixes all vertices of V^i and V^{i-1}. By Lemma 3.2.10, the conclusion follows. □

Theorem 3.2.15 *Let m and n be odd, $m \geq 3$. Let $M = M(\alpha; m, n)$ have coiled girth m and be loosely coiled. Then M is $\frac{1}{2}$-transitive.*

PROOF. By Lemmas 3.2.14 and 3.2.12, either $\mathrm{Aut}(M) = \langle \rho, \tau, \pi \rangle$ or $|\mathrm{Aut}(M)| = 2|\langle \rho, \tau, \pi \rangle|$. Suppose M is arc-transitive. Then, by the Orbit-Stabilizer Theorem, $4mn$ divides $|\mathrm{Aut}(M)|$ so that, by the previous statement, $|\mathrm{Aut}(M)| = 4mn$. Also, there exists $\sigma \in \mathrm{Aut}(M)$ that interchanges two adjacent vertices of M. Without loss of generality we may assume that these two vertices are v_0^0 and v_1^1. Clearly, $\sigma \notin \langle \rho, \tau, \pi \rangle$ since otherwise $\langle \rho, \tau, \pi \rangle$ would act transitively on the arcs of M. Hence $\mathrm{Aut}(M) = \langle \rho, \tau, \pi, \sigma \rangle$ and, by Lemma 3.2.14, σ has order 2.

Since σ interchanges v_0^0 and v_1^1, it interchanges the sets $\{v_{-1}^1, v_{\alpha^m}^{m-1}, v_{-\alpha^m}^{m-1}\}$ and $\{v_2^0, v_{1+\alpha}^2, v_{1-\alpha}^2\}$ of their neighbours. Now, the triples $v_0^0\, v_1^1\, v_{1+\alpha}^2$, $v_0^0\, v_1^1\, v_{1-\alpha}^2$, $v_1^1\, v_0^0\, v_{-\alpha^m}^{m-1}$, and $v_1^1\, v_0^0\, v_{\alpha^m}^{m-1}$ are contained in m-cycles but $v_2^0\, v_1^1\, v_0^0$ and $v_{-1}^1\, v_0^0\, v_1^1$ are not, so that σ must interchange v_{-1}^1 and v_2^0. Continuing in this fashion along the $2n$-cycle $M[V^0, V^1]$ (beginning with v_{-1}^1 and v_2^0 and their neighbours), we see that σ interchanges V^0 and V^1. Consequently, σ interchanges V^{m-1} and V^2, V^{m-2} and V^3, and so on. Thus $\mathrm{Aut}(M) = \langle \rho, \tau, \pi, \sigma \rangle$ acts imprimitively with the orbits of ρ as blocks.

It is not difficult to see that the action of σ on the vertices of $M[V^0, V^1]$ is in fact given by $\sigma(v_j^i) = v_{-j+1}^{-i+1}$. Hence for any $v_j^i \in V^0 \cup V^1$,

$$\sigma\rho\sigma(v_j^i) = \sigma\rho(v_{-j+1}^{-i+1}) = \sigma(v_{-j+2}^{-i+1}) = v_{j-1}^i = \rho^{-1}(v_j^i),$$

implying that the restriction of $\sigma\rho\sigma$ to $M[V^0, V^1]$ is the restriction of ρ^{-1}. Thus the restriction of $(\sigma\rho)^2$ to $M[V^0, V^1]$ is the identity so that, by Lemma 3.2.10, $(\sigma\rho)^2$ is the identity. Notice also that

$$\pi\rho\pi(v_j^i) = \pi\rho(v_{-j}^i) = \pi(v_{-j+1}^i) = v_{j-1}^i = \rho^{-1}(v_j^i)$$

so that $\pi\rho\pi = \rho^{-1}$. But then

$$(\sigma\pi)\rho(\sigma\pi)^{-1} = \sigma\pi\rho\pi^{-1}\sigma^{-1} = \sigma^{-1}\pi\rho\pi\sigma^{-1} = \sigma^{-1}\rho^{-1}\sigma^{-1} = (\sigma\rho\sigma)^{-1} = \rho,$$

so $\sigma\pi$ commutes with ρ.

Clearly, the action of $\sigma\pi$ on the orbits of ρ is identical to the action of σ. Thus, since m is odd, there is an orbit V^i of ρ which is fixed by $\sigma\pi$. We determine the action of $\sigma\pi$ on the vertices of V^i as follows. Let $\sigma\pi(v_0^i) = v_k^i$. Then, since $\sigma\pi$ commutes with ρ, $\sigma\pi(v_1^i) = \sigma\pi\rho(v_0^i) = \rho\sigma\pi(v_0^i) = v_{k+1}^i$. Inductively, we obtain $\sigma\pi(v_j^i) = v_{j+k}^i$ so that the action of $\sigma\pi$ on V^i is the same as that of ρ^k. Let $\gamma = \sigma\pi\rho^{-k}$. Then γ fixes the block V^i pointwise. Hence by Lemma 3.2.11, γ is the identity and thus $\sigma = \rho^k\pi$. But then $\sigma \in \langle\rho, \tau, \pi\rangle$, a contradiction.

Thus M is $\frac{1}{2}$-transitive. □

In general, it is not easy to determine for which values of the parameters α, m, and n the graph $M(\alpha; m, n)$ has coiled girth m and is loosely coiled. In [2], the authors propose the following sufficient condition: n is prime and α is a divisor of $n-1$ whose order m is odd and composite. We extend this condition in the next corollary.

Corollary 3.2.16 *Let p be an odd prime such that $p - 1 = km'd$ where $m', d > 1$ are odd. Let $n = p^s$ for some $s \in N$ and let $\alpha \in Z_n^*$ have order $m = m'dp^{s-1}$. Then the graph $M = M(\alpha; m, n)$ is $\frac{1}{2}$-transitive.*

PROOF. First notice that the group Z_n^* is cyclic by Theorem 1.0.11 so that, since m divides $\varphi(n) = (p-1)p^{s-1}$, there exists $\alpha \in Z_n^*$ with order m.

Next we show that $\alpha^d - 1$ can not be a zero divisor in the ring Z_n. Assume the contrary. Then $\alpha^{td} - 1$ is a zero divisor for all $t \in \{1, 2, \ldots, m'p^{s-1} - 1\}$ because $\alpha^d - 1$ divides $\alpha^{td} - 1$. Since the order of α is m, the elements $\alpha^{td} - 1$, $t = 1, 2, \ldots, m'p^{s-1} - 1$, are pairwise distinct. We would thus have $m'p^{s-1} - 1 > p^{s-1} - 1$ zero divisors in Z_n, a contradiction.

Hence $\alpha^d - 1 \in Z_n^*$ and, consequently, $\alpha - 1 \in Z_n^*$. Therefore, $\alpha^m \equiv 1 \pmod n$ implies

$$1 + \alpha^d + \alpha^{2d} + \ldots + \alpha^{(\frac{m}{d}-1)d} \equiv 0 \pmod n \tag{3.9}$$

and

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{m-1} \equiv 0 \pmod{n}. \tag{3.10}$$

Because of congruence (3.10),

$$C = v_0^0 \, v_1^1 \, v_{1+\alpha}^2 \, v_{1+\alpha+\alpha^2}^3 \, \cdots \, v_{1+\alpha+\ldots+\alpha^{m-2}}^{m-1} \, v_0^0$$

is a coiled m-cycle so that M has coiled girth m. From equations (3.9) and (3.10) we obtain

$$-1+\alpha+\ldots+\alpha^{d-1}-\alpha^d+\alpha^{d+1}\ldots+\alpha^{2d-1}-\alpha^{2d}+\alpha^{2d+1}+\ldots+\alpha^{m-1} \equiv 0 \pmod{n}.$$

This equation gives rise to a coiled m-cycle which does not appear in the ρ-partition of M induced by C. Hence M is loosely coiled and thus $\frac{1}{2}$-transitive by Theorem 3.2.15. □

The corollary we have just proved implies that whenever n is a prime of the form $9k + 1$ and $\alpha \in Z_n^*$ has order 9, $M(\alpha; 9, n)$ is $\frac{1}{2}$-transitive. Since by Dirichlet's Theorem 1.0.12 there are infinitely many primes of the form $9k+1$, there are infinitely many $\frac{1}{2}$-transitive graphs of degree 4. Three more infinite families of $\frac{1}{2}$-transitive graphs of degree 4 will be found in the next two sections.

3.3 Metacirculant graphs $M(\alpha; 3, n)$

In the previous section, the general case for m and n odd is covered when $M(\alpha; m, n)$ has coiled girth m and is loosely coiled. The other cases are covered in this section, but only for $m = 3$. The results we prove here appear in [2]. However, we present a new proof for Lemma 3.3.2, which substitutes for Lemmas 4.1 and 4.2 in [2].

Throughout this section we assume that n is odd and that $m = 3$. Recall that the order of α is either 3 or 6 so that either $\alpha^3 \equiv 1 \pmod{n}$ or $\alpha^3 \equiv -1 \pmod{n}$. Since $\alpha^3 \equiv -1 \pmod{n}$ implies $(-\alpha)^3 \equiv 1 \pmod{n}$, and since the graphs $M(\alpha; 3, n)$ and $M(-\alpha; 3, n)$ are isomorphic, we may as well assume that α has order 3.

Lemma 3.3.2 has the same conclusion as Lemma 3.2.14, except that now we do not need the assumption that the graph is loosely coiled and this requires a completely different proof. The approach we use here (unlike in [2]) is an algebraic classification of all 6-cycles in the graph $M(\alpha; 3, n)$. (An equivalent method will be used in Section 3.4 for the graphs $M(\alpha; 4, n)$.) First we need a set of definitions.

Definitions 3.3.1 Let $a \in \{m, 2m\}$ be the order of α in Z_n^*. Let $P = v_{j_0}^{i_0} v_{j_1}^{i_1} \ldots v_{j_k}^{i_k}$ be a path in $M(\alpha; m, n)$ and let $\Delta_l \in \{\pm\alpha^i : i = 0, 1, \ldots, a-1\}$ for $l = 0, 1, \ldots, k-1$. If $\Delta_l = j_{l+1} - j_l$ for $l = 0, 1, \ldots, k-1$, then

$$\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$$

is called a *jump sequence* of the path P. Notice that if $\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$ is a jump sequence of a given path, then so is $\langle -\Delta_{k-1}, \ldots, -\Delta_1, -\Delta_0 \rangle$. In addition, if $v_{j_0}^{i_0} = v_{j_k}^{i_k}$, that is, if P is a cycle, then cyclically permuting the entries in $\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$ yields another jump sequence for P. We shall not distinguish between jump sequences of the same path or cycle. Furthermore, if $\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$ is a jump sequence of a cycle, then

$$\Delta_0 + \Delta_1 + \ldots + \Delta_{k-1} \equiv 0 \pmod{n}$$

must hold. This is the *congruence equality* associated with the jump sequence $\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$.

If $\langle \Delta_0, \Delta_1, \ldots, \Delta_{k-1} \rangle$ is a jump sequence for the path P, then for any $s \in \{0, 1, \ldots, a-1\}$ and any $\delta \in \{-1, 1\}$,

$$\langle \delta\alpha^s \Delta_0, \delta\alpha^s \Delta_1, \ldots, \delta\alpha^s \Delta_{k-1} \rangle$$

will be called a *type sequence* of the path P. Two type sequences will be called *equivalent* if one can be obtained from the other by cyclically permuting the entries (for cycles only), reversing the order and/or the signs of the entries, and/or multiplying all entries by the same power of α. In other words, all type sequences of the same path or cycle are equivalent. Notice that, for cycles, equivalent type sequences give equivalent congruence equalities in the sense that they differ only by a factor of $\pm\alpha^i$.

The sequence $\langle\langle i_0, i_1, \ldots, i_{k-1}, i_k \rangle\rangle$ or $\langle\langle i_0, i_1, \ldots, i_{k-1} \rangle\rangle$ will be referred to as a *block sequence* of the path or cycle, respectively, $P = v_{j_0}^{i_0} v_{j_1}^{i_1} \ldots v_{j_{k-1}}^{i_{k-1}} v_{j_k}^{i_k}$. Notice that for two block sequences of the same cycle, one can be obtained from the other by cyclically permuting the entries and/or reversing their order. We shall not distinguish between block sequences of the same cycle.

Lemma 3.3.2 *Let $n \geq 9$ be odd and let $\alpha \in Z_n^*$ have order 3. Then every automorphism of $M = M(\alpha; 3, n)$ that fixes two adjacent vertices is the identity.*

PROOF. The Holt graph $M(4; 3, 9)$ plays a special role in this proof. We therefore first observe that the graphs $M(\alpha; 3, 9)$ are isomorphic for all $\alpha \in Z_9^*$ of order 3. Well, if α and α_1 are two order-three elements of Z_9^*, then $\alpha_1 \equiv \alpha^2 \pmod 9$. Define a mapping σ from $M(\alpha; 3, 9)$ to $M(\alpha^2; 3, 9)$ by $\sigma(v_j^i) = v_j^{-i+1}$. Since $\alpha^i \equiv (\alpha^2)^{-i}$ (mod 9) for $i = 0, 1, 2$, we have

$$\sigma(v_j^i \, v_{j \pm \alpha^i}^{i+1}) = v_j^{-i+1} \, v_{j \pm \alpha^i}^{-i} = v_j^{-i+1} \, v_{j \pm (\alpha^2)^{-i}}^{-i}$$

so that σ is an isomorphism. We may therefore assume that $\alpha = 4$ whenever $n = 9$.

Next we would like to classify all 6-cycles in M. It is not difficult to see that the following are the only possible non-equivalent block sequences of a 6-cycle in $M(\alpha; 3, n)$:

(A) $\langle\!\langle i, i+1, i+2, i, i+1, i+2\rangle\!\rangle$,
(B) $\langle\!\langle i, i+1, i+2, i, i+2, i+1\rangle\!\rangle$,
(C) $\langle\!\langle i, i+1, i+2, i+1, i+2, i+1\rangle\!\rangle$,
(D) $\langle\!\langle i, i+1, i, i+1, i+2, i+1\rangle\!\rangle$, and
(E) $\langle\!\langle i, i+1, i, i+1, i, i+1\rangle\!\rangle$.

We examine the equations associated with these block sequences. Throughout this proof, let $\delta, \delta_i, \delta_i' \in \{-1, 1\}$ for $i = 0, 1, 2$.

The block sequences (A) and (B) are associated with the type sequences $\langle \delta_0, \delta_1\alpha, \delta_2\alpha^2, \delta_0', \delta_1'\alpha, \delta_2'\alpha^2\rangle$ and $\langle \delta_0, \delta_1\alpha, \delta_2\alpha^2, \delta_2'\alpha^2, \delta_1'\alpha, \delta_0\rangle$, respectively. In both cases, the equation associated with the cycle has the form

$$(\delta_0 + \delta_0') + (\delta_1 + \delta_1')\alpha + (\delta_2 + \delta_2')\alpha^2 \equiv 0 \pmod{n}.$$

Since n is odd, this may be reduced to

$$\varepsilon_0 + \varepsilon_1\alpha + \varepsilon_2\alpha^2 \equiv 0 \pmod{n},$$

where $\varepsilon_i = \frac{1}{2}(\delta_i + \delta_i') \in \{-1, 0, 1\}$ for $i = 0, 1, 2$. Suppose that none of $\varepsilon_0, \varepsilon_1, \varepsilon_2$ is zero. Then $\varepsilon_i = \delta_i$ for all i, so that a subpath of the 6-cycle is a 3-cycle, which is impossible. Hence at least one of the ε_i is zero. Notice that it can not happen that exactly two of the ε_i are zero. Hence either $\varepsilon_i = 0$ for all i or exactly one of the ε_i is zero. The latter possibility implies either $1 + \delta\alpha \equiv 0 \pmod{n}$ or $1 + \delta\alpha^2 \equiv 0 \pmod{n}$, both contradicting the fact that the order of α is 3.

Hence $\varepsilon_i = 0$ and $\delta_i' = -\delta_i$ for all $i = 0, 1, 2$. Since the block sequence (B) requires $\delta_2' = \delta_2$, the only type sequences we obtain from this are of the form

$$\langle 1, \delta_1\alpha, \delta_2\alpha^2, -1, -\delta_1\alpha, -\delta_2\alpha^2\rangle.$$

The block sequence (C) requires a type sequence of the form $\langle 1, \delta\alpha, \delta\alpha, \delta\alpha, \delta\alpha, 1\rangle$ so the equation is $2 + 4\delta\alpha \equiv 0 \pmod{n}$, that is, $2\delta\alpha \equiv -1 \pmod{n}$. Cubing both sides we obtain $8\delta \equiv -1 \pmod{n}$ so that $n \in \{3, 7, 9\}$. Since we have assumed that

$n \geq 9$, we must have $n = 9$. The corresponding multiplier is $\alpha = 4$ but then the equation is satisfied only for $\delta = 1$. We thus obtain the type sequence

$$\langle 1, \alpha, \alpha, \alpha, \alpha, 1 \rangle,$$

where $\alpha = 4$ and $n = 9$.

The block sequence (D) requires $4 + 2\delta\alpha \equiv 0 \pmod{n}$. This implies $n \in \{3, 7, 9\}$. Hence $n = 9$. But the equation can not be satisfied for $\alpha = 4$.

The block sequence (E) implies $6 \equiv 0 \pmod{n}$, clearly impossible.

With the information we have gathered, the proof splits into three cases.

Case 1. M has coiled girth 3.
Since M has coiled girth 3, at least one of the equations $\alpha^2 + \alpha + 1 \equiv 0 \pmod{n}$, $\alpha^2 + \alpha - 1 \equiv 0 \pmod{n}$, and $\alpha^2 - \alpha - 1 \equiv 0 \pmod{n}$ must hold. In fact, exactly one of these equations holds since otherwise we would have either $2 \equiv 0 \pmod{n}$, $2\alpha \equiv 0 \pmod{n}$, or $2(\alpha + 1) \equiv 0 \pmod{n}$. Since $\alpha^3 \equiv 1 \pmod{n}$, $(\alpha - 1)(\alpha^2 + \alpha + 1) \equiv 0 \pmod{n}$. This implies that either $\alpha^2 + \alpha + 1 \equiv 0 \pmod{n}$ or $\alpha^2 + \alpha + 1$ is a zero divisor in Z_n. If $\alpha^2 + \alpha + 1$ is a zero divisor, then $\alpha^2 + \alpha + 1 \not\equiv 2 \pmod{n}$ because 2 is not a zero divisor in Z_n when n is odd. Hence $\alpha^2 + \alpha - 1 \not\equiv 0 \pmod{n}$. Therefore, since M has coiled girth 3, either $\alpha^2 + \alpha + 1 \equiv 0 \pmod{n}$ or $\alpha^2 - \alpha - 1 \equiv 0 \pmod{n}$ (but not both) must hold. In either case, each edge of M lies in a unique 3-cycle. Notice that for $n = 9$ and $\alpha = 4$ none of these two congruences holds so that $M(4; 3, 9)$ has coiled girth 6. Hence, when M has coiled girth 3, all 6-cycles in M have a block sequence (A), that is, they are coiled.

Let σ be an automorphism of M that fixes the vertices v_0^0 and v_1^1. First assume that $\alpha^2 + \alpha + 1 \equiv 0 \pmod{n}$. Then $v_0^0 v_1^1 v_{1+\alpha}^2$ is a 3-cycle so that σ fixes $v_{1+\alpha}^2$. Suppose that σ interchanges the other two neighbours of v_1^1, that is, v_2^0 and $v_{1-\alpha}^2$. But the triple $v_0^0 v_1^1 v_{1-\alpha}^2$ lies in a 6-cycle while $v_0^0 v_1^1 v_2^0$ does not. Hence σ fixes v_2^0 and $v_{1-\alpha}^2$ as well. Continuing in this way, since n is odd, establishes that V^0 and V^1 are fixed pointwise. Hence by Lemma 3.2.10, σ is the identity.

The case when $\alpha^2 - \alpha - 1 \equiv 0 \pmod{n}$ is done in a very similar way.

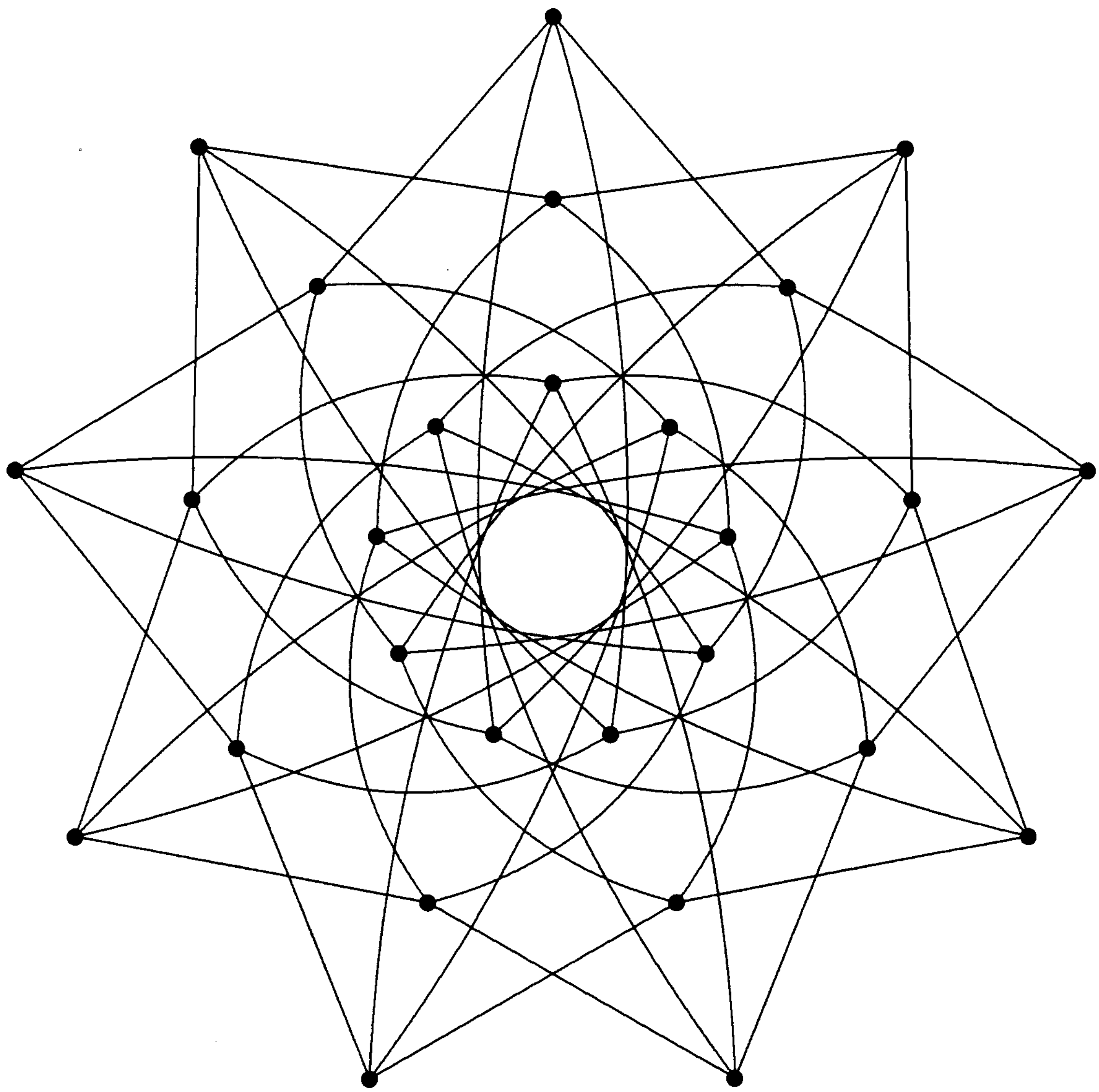

Figure 3.3: The Holt graph $M(4;3,9)$

Case 2. M has coiled girth 6 and $n > 9$.
Suppose $\sigma \in \mathrm{Aut}(M)$ fixes the vertices v_0^0 and v_1^1. Notice that M contains no non-coiled 6-cycles while each 2-path with a block sequence $\langle\langle i, i+1, i+2\rangle\rangle$ lies in exactly two coiled 6-cycles. Hence σ fixes v_2^0 in addition to fixing v_0^0 and v_1^1. Continuing in this way, since n is odd, we see that σ fixes V^0 and V^1 pointwise. Hence σ is the identity.

Case 3. Holt's graph $M = M(4; 3, 9)$.
First observe the following. A 2-path with a type sequence $\langle 1, 1\rangle$ and a block sequence $\langle\langle i+1, i, i+1\rangle\rangle$ lies in exactly two 6-cycles. In particular, for a 2-path with a jump sequence $\langle 1, 1\rangle$ and block sequence $\langle\langle i+1, i, i+1\rangle\rangle$ these two 6-cycles have jump sequences $\langle 1, \alpha, \alpha, \alpha, \alpha, 1\rangle$ and $\langle \alpha^2, 1, 1, 1, 1, \alpha^2\rangle$, respectively. The same is true of a 2-path with a type sequence $\langle 1, 1\rangle$ and a block sequence $\langle\langle i, i+1, i\rangle\rangle$, except that for a 2-path with a jump sequence $\langle 1, 1\rangle$ and a block sequence $\langle\langle i, i+1, i\rangle\rangle$ both 6-cycles have a jump sequence $\langle \alpha^2, 1, 1, 1, 1, \alpha^2\rangle$. Further, a 2-path with a type sequence $\langle -\alpha^2, 1\rangle$ lies in exactly two 6-cycles, both of which are coiled, while a 2-path with a type sequence $\langle \alpha^2, 1\rangle$ lies in exactly three 6-cycles, two of which are coiled. For example, a 2-path with a jump sequence $\langle \alpha^2, 1\rangle$ lies in 6-cycles with jump sequences $\langle 1, \alpha, -\alpha^2, -1, -\alpha, \alpha^2\rangle$, $\langle 1, -\alpha, -\alpha^2, -1, \alpha, \alpha^2\rangle$, and $\langle \alpha^2, 1, 1, 1, 1, \alpha^2\rangle$.

Now let σ be an automorphism of M that fixes the vertices v_0^0 and v_1^1. Since the 2-paths $v_{-1}^1\, v_0^0\, v_1^1$ and $v_{\alpha^2}^2\, v_0^0\, v_1^1$ lie in exactly two 6-cycles each, while the 2-path $v_{-\alpha^2}^2\, v_0^0\, v_1^1$ lies in three 6-cycles, σ fixes $v_{-\alpha^2}^2$. The three 6-cycles containing $v_{-\alpha^2}^2\, v_0^0\, v_1^1$ are

$$C_1 = v_{-\alpha^2}^2\, v_0^0\, v_1^1\, v_{1+\alpha}^2\, v_{1+\alpha-\alpha^2}^0\, v_{\alpha-\alpha^2}^1\, v_{-\alpha^2}^2,$$

$$C_2 = v_{-\alpha^2}^2\, v_0^0\, v_1^1\, v_{1-\alpha}^2\, v_{1-\alpha-\alpha^2}^0\, v_{-\alpha-\alpha^2}^1\, v_{-\alpha^2}^2, \text{ and}$$

$$C_3 = v_{-\alpha^2}^2\, v_0^0\, v_1^1\, v_2^0\, v_3^1\, v_4^0\, v_{-\alpha^2}^2.$$

Hence $\sigma(v_2^0) \in \{v_2^0, v_{1+\alpha}^2, v_{1-\alpha}^2\}$. Now $v_0^0\, v_1^1\, v_2^0$ lies in exactly two 6-cycles while $v_0^0\, v_1^1\, v_{1+\alpha}^2$ lies in three 6-cycles because it has a type sequence $\langle \alpha^2, 1\rangle$. Thus $\sigma(v_2^0) \neq v_{1+\alpha}^2$. If $\sigma(v_2^0) = v_{1-\alpha}^2$, then $\sigma(C_3) = C_2$ so that $\sigma(v_4^0) = v_{-\alpha-\alpha^2}^1$. But $v_4^0\, v_{-\alpha^2}^2\, v_0^0$

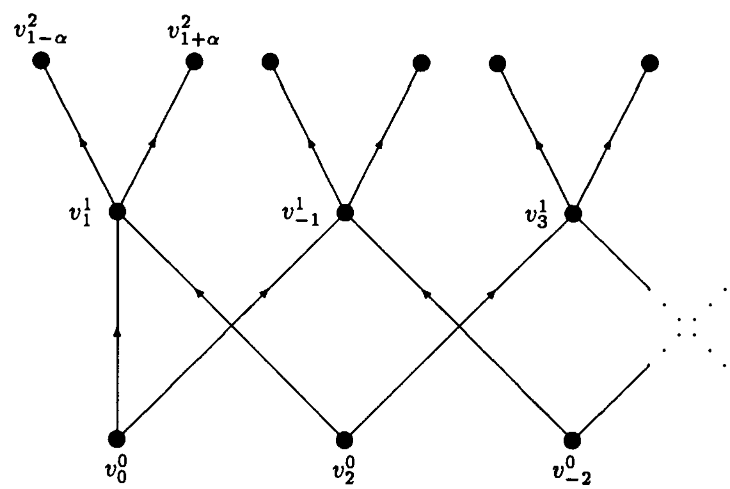

Figure 3.4: Theorem 3.3.3

lies in exactly two 6-cycles (type sequence $\langle 1,1\rangle$) while $v^1_{-\alpha-\alpha^2}\, v^2_{-\alpha^2}\, v^0_0$ lies in three 6-cycles, a contradiction. Thus the only possibility is that σ fixes v^0_2. Continuing in this way along the 18-cycle $M[V^0, V^1]$ and using Lemma 3.2.10 establishes the result. $\square$

Theorem 3.3.3 *Let $n \geq 9$ be odd and let $\alpha \in Z^*_n$ have order 3. The graph $M = M(\alpha; 3, n)$ is $\frac{1}{2}$-transitive.*

Proof. Suppose M is arc-transitive. Then there exists $\sigma \in \mathrm{Aut}(M)$ that interchanges the vertices v^0_0 and v^1_1. By Lemma 3.3.2, σ has order 2. The group $\langle \rho, \tau, \pi \rangle$ acts transitively on the edges of M, but not on the arcs of M because $|\langle \rho, \tau, \pi \rangle| = 6n$. Hence $\sigma \notin \langle \rho, \tau, \pi \rangle$ and, by Lemma 3.2.12, $|\mathrm{Aut}(M)| = |\langle \rho, \tau, \pi, \sigma \rangle| = 2|\langle \rho, \tau, \pi \rangle|$. Thus $\mathrm{Aut}(M) = \langle \rho, \tau, \pi \rangle \cup \sigma\langle \rho, \tau, \pi \rangle = \langle \rho, \tau, \pi \rangle \cup \langle \rho, \tau, \pi \rangle\sigma$, that is, $\langle \rho, \tau, \pi \rangle$ is normal in $\mathrm{Aut}(M)$.

Orient the edge $v^0_0 v^1_1$ from v^0_0 to v^1_1 obtaining the arc $a = (v^0_0, v^1_1)$. The group $\langle \rho, \tau, \pi \rangle$ acting on (v^0_0, v^1_1) gives an orientation of M which we denote by M^*. The group $\langle \rho, \tau, \pi \rangle$ acts transitively on the arcs of M^* and since $|\langle \rho, \tau, \pi \rangle| = 6n = |A(M^*)|$, $\langle \rho, \tau, \pi \rangle$ acts regularly on the arcs of M^*. This means that for any arc b of

M^* there exists a unique $f_b \in \langle \rho, \tau, \pi \rangle$ such that $f_b(a) = b$. Then $\sigma(b) = \sigma f_b(a) = f_c\sigma(a)$ for a unique $c \in A(M^*)$. Thus σ maps any arc of M^* to a reversed arc of M^* so that σ is orientation reversing on M^*. We now carefully examine the action of σ.

Notice that $(v_0^0, v_{-1}^1) = \pi(v_0^0, v_1^1)$, $(v_2^0, v_1^1) = \rho^2\pi(v_0^0, v_1^1)$, $(v_1^1, v_{1+\alpha}^2) = \rho\tau(v_0^0, v_1^1)$, and $(v_1^1, v_{1-\alpha}^2) = \rho\pi\tau(v_0^0, v_1^1)$ are arcs of M^*. Hence, since σ interchanges v_0^0 and v_1^1 and is orientation reversing, σ must also interchange v_{-1}^1 and v_2^0. Similarly, since (v_2^0, v_3^1) is an arc of M^*, and (v_{-2}^0, v_{-1}^1) is the only arc of M^* whose terminal vertex is v_{-1}^1, σ interchanges v_3^1 and v_{-2}^0. Continuing in this way, we see that σ must interchange v_k^1 and v_{-k+1}^0 for all $k \in Z_n$. Hence V^2 is fixed setwise.

Now v_1^1 and $v_{1+2\alpha}^1$ have the common neighbour $v_{1+\alpha}^2$ in V^2. Thus v_0^0 and $v_{-2\alpha}^0 = \sigma(v_{1+2\alpha}^1)$ have a common neighbour in V^2. But then $2\alpha \equiv \pm 2\alpha^2 \pmod n$ implying $\alpha \equiv \pm 1 \pmod n$, which contradicts the assumption that the order of α is 3.

Therefore no such σ exists and M is $\frac{1}{2}$-transitive as required. □

Since a graph $M(\alpha; 3, n)$ exists for every prime n of the form $3k + 1$, we now know that there are infinitely many $\frac{1}{2}$-transitive graphs $M(\alpha; 3, n)$. In particular, we have proved that the graph $M(4; 3, 9)$ is $\frac{1}{2}$-transitive. This graph was named after D. F. Holt [8] who discovered it in 1981 (clearly, not as a metacirculant), although it was not until recently that Alspach, Marušič, and Nowitz [2] have shown that this graph is a $\frac{1}{2}$-transitive graph of smallest degree and with the smallest number of vertices (Theorem 2.1.8). In addition, they have asked how many $\frac{1}{2}$-transitive graphs of order 27 and degree 4 there are up to isomorphism. This question was answered by Xu in the following form [17].

Theorem 3.3.4 *For any odd prime p there are, up to isomorphism, precisely $\frac{p-1}{2}$ $\frac{1}{2}$-transitive graphs of order p^3 and degree 4. They are all metacirculants.*

We therefore have

Corollary 3.3.5 *Up to isomorphism there is only one $\frac{1}{2}$-transitive graph of order 27 and degree 4, namely, the Holt graph.*

3.4 Metacirculant graphs $M(\alpha; 4, n)$

In the previous two sections we have been able to establish $\frac{1}{2}$-transitivity of certain graphs $M(\alpha; m, n)$ only with the condition that both m and n are odd. In this section we present new results concerning $\frac{1}{2}$-transitivity of the metacirculant graphs $M(\alpha; 4, n)$. The approach we use here is classification of 8-cycles in $M(\alpha; 4, n)$ with respect to their block sequences. The only case when we shall not be able to establish either arc-transitivity or $\frac{1}{2}$-transitivity of the graphs $M(\alpha; 4, n)$ is when the order of α is 4 and either n is a multiple of 5 but not a prime power or n is a multiple of 4. In addition, we will show that the graphs $M(\alpha; 2, n)$ are arc-transitive.

We begin with a couple of lemmas concerning general graphs $M(\alpha; m, n)$.

Lemma 3.4.1 *Let $n \equiv 0 \pmod 4$ and $\alpha \in Z_n^*$. If $\alpha^m \equiv -1 \pmod n$, then m is odd and $\alpha \equiv 3 \pmod 4$. If $\alpha^m \equiv 1 \pmod n$, then m is even or $\alpha \equiv 1 \pmod 4$.*

PROOF. Since $\alpha \in Z_n^*$ and n is even, α must be odd. Let $\alpha = 2k + 1$ for some $k \in Z_n$.

If $\alpha^m \equiv -1 \pmod n$, then $\alpha^m + 1 \equiv 0 \pmod 4$. Thus we have

$$0 \equiv \alpha^m + 1 \equiv (2k+1)^m + 1 \equiv 2mk + 2 \equiv 2(mk+1) \pmod 4$$

so that m and k must both be odd. Hence also $\alpha \equiv 3 \pmod 4$.

If $\alpha^m \equiv 1 \pmod n$, then $\alpha^m - 1 \equiv 0 \pmod 4$. We have

$$0 \equiv \alpha^m - 1 \equiv (2k+1)^m - 1 \equiv 2mk \pmod 4.$$

Hence at least one of m and k must be even. Therefore either m is even or $\alpha \equiv 1 \pmod 4$ or both. ∎

Lemma 3.4.2 *Let n be even. Then $M(\alpha; m, n)$ is connected if and only if m is odd. If $n \equiv 2 \pmod 4$ and m is even, then $M(\alpha; m, n)$ consists of two connected components which are both isomorphic to $M(\alpha \bmod \frac{n}{2}; m, \frac{n}{2})$*

PROOF. Since n is even, α is odd and $M[V^i, V^{i+1}]$ consists of two disjoint n cycles. One cycle alternates between vertices of V^i with odd subscripts and vertices of V^{i+1} with even subscripts, and the other cycle alternates between vertices of V^i with even subscripts and vertices of V^{i+1} with odd subscripts. It is now clear that $M(\alpha; m, n)$ is connected if and only if m is odd.

Now let $n \equiv 2 \pmod 4$ and let m be even. Then we get exactly two components and $\rho(v_j^i) = v_{j+1}^i$ is an isomorphism between them. Choose the component with vertex set $V' = \{v_j^i : i \in Z_m, j \in Z_n, i \equiv j \,(\mathrm{mod}\ 2)\}$ and let V_k be the vertex set of the graph $M(\alpha \bmod k; m, k)$, where $k = \frac{n}{2}$. Define $\sigma : V' \to V_k$ by $\sigma(v_j^i) = v_{j \bmod k}^i$. Since each of the sets $\{0, 2, \ldots. n-2\}$ and $\{1, 3, \ldots, n-1\}$ modulo k produces all of Z_k, σ is a bijection. Since also $l - j \equiv \alpha^i \pmod n$ implies $(l \bmod k) - (j \bmod k) \equiv (\alpha \bmod k)^i \pmod k$ for any $j, l \in Z_n$, $i \in Z_m$, σ is an isomorphism between the connected component of $M(\alpha; m, n)$ with vertex set V' and $M(\alpha \bmod k; m, k)$. □

Theorem 3.4.3 *If the order of α is 4 and $\alpha^2 \equiv -1 \pmod n$, then $M(\alpha; 4, n)$ is arc-transitive.*

PROOF. Define $\sigma(v_j^i) = v_{-j+1}^{-i+1}$. Since the order of α is 4 and $\alpha^2 \equiv -1 \pmod n$, $\alpha^2 \equiv \alpha^{-2} \pmod n$ and $\alpha \equiv -\alpha^{-1} \pmod n$. Hence, for any $\delta \in \{-1, 1\}$, we have

$$\sigma(v_j^i v_{j+\delta\alpha^i}^{i+1}) = v_{-j+1}^{-i+1} v_{-j+1-\delta\alpha^i}^{-i} = \begin{cases} v_{-j+1}^{-i+1} v_{-j+1-\delta\alpha^{-i}}^{-i} & \text{if } i \in \{0, 2\} \\ v_{-j+1}^{-i+1} v_{-j+1+\delta\alpha^{-i}}^{-i} & \text{if } i \in \{1, 3\} \end{cases}$$

so that σ is an automorphism of $M(\alpha; 4, n)$. Since σ interchanges the endpoints of the edge $v_0^0 v_1^1$, $M(\alpha; 4, n)$ is arc-transitive. □

Corollary 3.4.4 *Let p be an odd prime, $n = p^k$ for some $k \in N$, and $\alpha \in Z_n^*$ have order 4. Then $M(\alpha; 4, n)$ is arc-transitive.*

PROOF. Since n is an odd prime power, Z_n^* is cyclic by Theorem 1.0.11. Therefore, since the order of α is 4, $\alpha^2 \equiv -1 \pmod n$. The result now follows from Theorem 3.4.3. □

As a by-product, the same automorphism as in the proof of Theorem 3.4.3 works in proving the following statement.

Theorem 3.4.5 *$M(\alpha; 2, n)$ is arc-transitive.*

PROOF. With σ defined as in the proof of Theorem 3.4.3, we have

$$\sigma(v_j^i v_{j+\delta\alpha^i}^{i+1}) = v_{-j+1}^{-i+1} v_{-j+1-\delta\alpha^i}^{-i} = v_{-j+1}^{i+1} v_{-j+1-\delta\alpha^i}^{i}$$

because $i \equiv -i \pmod 2$. Thus σ is an automorphism of $M(\alpha; 2, n)$ that reverses the edge $v_0^0 v_1^1$. □

Lemma 3.4.6 *Let n be a prime. If $\alpha_1, \alpha_2 \in Z_n^*$ both have order 8, then $M(\alpha_1; 4, n)$ and $M(\alpha_2; 4, n)$ are isomorphic.*

PROOF. If $\alpha \in Z_n^*$ is an element of order 8, then, since Z_n^* is cyclic, $\alpha^4 \equiv -1 \pmod n$ and all elements of Z_n^* of order 8 are α, α^3, $-\alpha$, and $-\alpha^3$. $M(\alpha; 4, n)$ and $M(-\alpha; 4, n)$ are clearly isomorphic with the identity mapping being an isomorphism. Now define a mapping from $M(\alpha; 4, n)$ to $M(\alpha^3; 4, n)$ by $\sigma(v_j^i) = v_j^{-i+1}$. Since $\alpha^i \equiv (\alpha^3)^{-i}$ for $i = 0, 2$, and $\alpha^i \equiv -(\alpha^3)^{-i} \pmod n$ for $i = 1, 3$, we have

$$\sigma(v_j^i v_{j+\delta\alpha^i}^{i+1}) = v_j^{-i+1} v_{j+\delta\alpha^i}^{-i} = v_j^{-i+1} v_{j\pm\delta(\alpha^3)^{-i}}^{-i}$$

so that σ is an isomorphism. This proves the lemma. □

Consequently, for any prime n it is enough to consider the graph $M(\alpha; 4, n)$ for one order-eight element α of Z_n^* only.

We proceed to explore 8-cycles in the graphs $M(\alpha; 4, n)$. Recall Definitions 3.3.1.

Lemma 3.4.7 *If n is odd, the order of α is 8 and $\alpha^4 \equiv -1 \pmod n$, then $M(\alpha; 4, n)$ has coiled girth 8. Furthermore, every coiled 8-cycle has a type sequence*

$$\langle 1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3, -1, -\delta_1\alpha, -\delta_2\alpha^2, -\delta_3\alpha^3 \rangle,$$

where $\delta_1, \delta_2, \delta_3 \in \{-1, 1\}$. All choices for the δ_i are realizable in the graph.

PROOF. First note that, since α has order 8, $\varphi(n)$ must be divisible by 8, where φ is the Euler φ-function.

We now show that $M(\alpha; 4, n)$ has coiled girth 8. Conversely, suppose that the graph contains a coiled 4-cycle with a type sequence

$$\langle 1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3 \rangle$$

for some $\delta_1, \delta_2, \delta_3 \in \{-1, 1\}$. Then

$$1 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n} \tag{3.11}$$

must hold. Expressing

$$\delta_2\alpha^2 \equiv -(1 + \delta_1\alpha + \delta_3\alpha^3) \pmod{n}$$

and then squaring both sides we obtain

$$-1 \equiv 1 + \alpha^2 - \alpha^2 + 2\delta_1\alpha + 2\delta_3\alpha^3 - 2\delta_1\delta_3 \pmod{n}$$

or

$$(2 - 2\delta_1\delta_3) + 2\delta_1\alpha + 2\delta_3\alpha^3 \equiv 0 \pmod{n}. \tag{3.12}$$

From equalities (3.11) and (3.12) we can eliminate the terms with α and α^3 simultaneously thus obtaining

$$2\delta_1\delta_3 + 2\delta_2\alpha^2 \equiv 0 \pmod{n}$$

or

$$-\delta_2\alpha^2 \equiv \delta_1\delta_3 \pmod{n}$$

since $\gcd(2, n) = 1$. Squaring both sides again yields $-1 \equiv 1 \pmod{n}$ which in turn implies $n = 2$, a contradiction. Hence $M(\alpha; 4, n)$ has coiled girth 8.

The above method will be called *squaring elimination.*

We now explore coiled 8-cycles. A coiled 8-cycle has a type sequence

$$\langle \delta_0', \delta_1'\alpha, \delta_2'\alpha^2, \delta_3'\alpha^3, \delta_0'', \delta_1''\alpha, \delta_2''\alpha^2, \delta_3''\alpha^3 \rangle$$

for some $\delta_i', \delta_i'' \in \{-1, 1\}$, $i = 0, \ldots, 3$, such that

$$\delta_0' + \delta_1'\alpha + \delta_2'\alpha^2 + \delta_3'\alpha^3 + \delta_0'' + \delta_1''\alpha + \delta_2''\alpha^2 + \delta_3''\alpha^3 \equiv 0 \pmod{n}$$

holds. This equation can be simplified to

$$\varepsilon_0 + \varepsilon_1\alpha + \varepsilon_2\alpha^2 + \varepsilon_3\alpha^3 \equiv 0 \pmod{n} \tag{3.13}$$

where $\varepsilon_i = \frac{1}{2}(\delta_i' + \delta_i'') \in \{-1, 0, 1\}$. We now apply the squaring elimination method described in the first part of the proof to (3.13) thus obtaining

$$-(\varepsilon_3^2 - \varepsilon_1^2 + 2\varepsilon_0\varepsilon_2)^2 \equiv (\varepsilon_0^2 - \varepsilon_2^2 + 2\varepsilon_1\varepsilon_3)^2 \pmod{n}.$$

The only posible values for $(\varepsilon_3^2 - \varepsilon_1^2 + 2\varepsilon_0\varepsilon_2)^2$ and $(\varepsilon_0^2 - \varepsilon_2^2 + 2\varepsilon_1\varepsilon_3)^2$ are 0,1,4, and 9. But whenever $-\varepsilon \equiv \varepsilon' \pmod{n}$ for $\varepsilon, \varepsilon' \in \{0, 1, 4, 9\}$ and at least one of ε and ε' is non-zero, $n \in \{3, 5, 9, 13\}$ is forced which is a contradiction. Hence $\varepsilon_3^2 - \varepsilon_1^2 + 2\varepsilon_0\varepsilon_2 = \varepsilon_0^2 - \varepsilon_2^2 + 2\varepsilon_1\varepsilon_3 = 0$, which implies $\varepsilon_i = 0$ for all $i = 0, \ldots, 3$. Therefore $\delta_i'' = -\delta_i'$ for $i = 0, \ldots, 3$, and the lemma is proved. $\square$

Next we state a result similar to that of Lemma 3.4.7 for the case that the order of α is 4. Notice that, by Theorem 3.4.3, we may assume that $\alpha^2 \not\equiv -1 \pmod{n}$ and hence that n is not an odd prime power.

Lemma 3.4.8 *Let n be odd with $n \not\equiv 0 \pmod{5}$ and let α have order 4 with $\alpha^2 \not\equiv -1 \pmod{n}$. If $M = M(\alpha; 4, n)$ has coiled girth 4, then (substituting α by $-\alpha$ if necessary) every coiled 4-cycle in M has a type sequence*

$$\langle 1, \alpha, \alpha^2, \alpha^3 \rangle.$$

Furthermore, every coiled 8-cycle has a type sequence of the form

$$\langle 1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3, -1, -\delta_1\alpha, -\delta_2\alpha^2, -\delta_3\alpha^3 \rangle,$$

where $\delta_1, \delta_2, \delta_3 \in \{-1, 1\}$. If M has coiled girth 8, all choices for δ_1, δ_2, and δ_3 are realizable. If M has coiled girth 4, all choices for δ_1, δ_2, and δ_3 are realizable except for $\delta_1 = \delta_2 = \delta_3 = 1$.

PROOF. First assume that M has coiled girth 4. Then either $\alpha^3+\alpha^2+\alpha+1 \equiv 0 \pmod n$, $\alpha^3+\alpha^2+\alpha-1 \equiv 0 \pmod n$, $\alpha^3+\alpha^2-\alpha-1 \equiv 0 \pmod n$, or $\alpha^3-\alpha^2+\alpha-1 \equiv 0 \pmod n$. Since $\alpha^4 \equiv 1 \pmod n$, either $\alpha^3+\alpha^2+\alpha+1 \equiv 0 \pmod n$ or $\alpha^3+\alpha^2+\alpha+1$ is a zero divisor in Z_n.

If $\alpha^3+\alpha^2+\alpha+1 \equiv 0 \pmod n$, then $\alpha^3+\alpha^2+\alpha-1 \not\equiv 0 \pmod n$ since $2 \not\equiv 0 \pmod n$, $\alpha^3+\alpha^2-\alpha-1 \not\equiv 0 \pmod n$ since $2(\alpha+1) \not\equiv 0 \pmod n$, and $\alpha^3-\alpha^2+\alpha-1 \not\equiv 0 \pmod n$ since $2(\alpha^2+1) \not\equiv 0 \pmod n$. Therefore every coiled 4-cycle has a type sequence $\langle 1, \alpha, \alpha^2, \alpha^3 \rangle$.

Now suppose that $\alpha^3+\alpha^2+\alpha+1$ is a zero divisor in Z_n. Since 2 is not a zero divisor, $\alpha^3+\alpha^2+\alpha-1 \not\equiv 0 \pmod n$. Suppose that $\alpha^3+\alpha^2-\alpha-1 \equiv 0 \pmod n$. Then $\alpha^3+\alpha^2+\alpha+1 \equiv 2(\alpha+1) \pmod n$ so that $0 \equiv \alpha^4-1 \equiv (\alpha-1)(\alpha^3+\alpha^2+\alpha+1) \equiv 2(\alpha-1)(\alpha+1) \equiv 2(\alpha^2-1) \pmod n$. Thus $\alpha^2 \equiv 1 \pmod n$, contradicting the assumption that the order of α is 4. Hence $\alpha^3-\alpha^2+\alpha-1 \equiv 0 \pmod n$ is the only possibility. But then $(-\alpha)^3+(-\alpha)^2+(-\alpha)+1 \equiv 0 \pmod n$. Therefore, since the graphs $M(\alpha;4,n)$ and $M(-\alpha;4,n)$ are isomorphic, we may assume that if $M(\alpha;4,n)$ has coiled girth 4, then $\alpha^3+\alpha^2+\alpha+1 \equiv 0 \pmod n$.

Next we explore coiled 8-cycles. As in the proof of the previous lemma, a coiled 8-cycle has a type sequence of the form

$$\langle \delta'_0, \delta'_1\alpha, \delta'_2\alpha^2, \delta'_3\alpha^3, \delta''_0, \delta''_1\alpha, \delta''_2\alpha^2, \delta''_3\alpha^3 \rangle$$

for some $\delta'_i, \delta''_i \in \{-1, 1\}$, $i = 0, \ldots, 3$, and this is associated with the equation

$$\varepsilon_0 + \varepsilon_1\alpha + \varepsilon_2\alpha^2 + \varepsilon_3\alpha^3 \equiv 0 \pmod n, \tag{3.14}$$

where $\varepsilon_i = \frac{1}{2}(\delta'_i + \delta''_i) \in \{-1, 0, 1\}$. Applying the squaring elimination method described in the proof of Lemma 3.4.7 and using $(\alpha^2)^2 \equiv 1 \pmod n$, (3.14) yields

$$(\varepsilon_1^2 + \varepsilon_3^2 - 2\varepsilon_0\varepsilon_2)\alpha^2 \equiv \varepsilon_0^2 + \varepsilon_2^2 - 2\varepsilon_1\varepsilon_3 \pmod n$$

and, squaring again,

$$(\varepsilon_1^2 + \varepsilon_3^2 - 2\varepsilon_0\varepsilon_2)^2 \equiv (\varepsilon_0^2 + \varepsilon_2^2 - 2\varepsilon_1\varepsilon_3)^2 \pmod n.$$

The only posible values for $\varepsilon = \varepsilon_1^2 + \varepsilon_3^2 - 2\varepsilon_0\varepsilon_2$ and $\varepsilon' = \varepsilon_0^2 + \varepsilon_2^2 - 2\varepsilon_1\varepsilon_3$ are $0, \pm 1, \pm 2$, 3, and 4. Thus whenever $\varepsilon^2 \equiv \varepsilon'^2 \pmod{n}$ and $\varepsilon^2 \neq \varepsilon'^2$, $n \in \{3, 5, 7, 9, 15\}$ is forced. But n is not a multiple of 5 nor is it a prime power so that we must have $\varepsilon^2 = \varepsilon'^2$. Consequently, $\varepsilon' = \pm\varepsilon$ so that $\varepsilon\alpha^2 \equiv \pm\varepsilon \pmod{n}$. This eliminates all possibilities except $\varepsilon = 0$ and $\varepsilon = 3$. If $\varepsilon = 3$, then $\varepsilon_0\varepsilon_2 \neq 0$ and hence ε' is even, contradicting the assumption $\varepsilon' = \pm\varepsilon$. Hence $\varepsilon = \varepsilon' = 0$. Now, if none of the ε_i is zero, then (3.14) implies that our coiled 8-cycle has a subpath which is a coiled 4-cycle, clearly impossible. It is now easy to see that we must have $\varepsilon_i = 0$ for all i and the conclusion follows. □

We would now like to classify the non-coiled 8-cycles in $M(\alpha; 4, n)$. It is not difficult to check that the following are the only possible block sequences for a non-coiled 8-cycle:

(a) $\langle\langle i, i+1, i+2, i+1, i, i+1, i+2, i+1 \rangle\rangle$,
(b) $\langle\langle i, i+1, i+2, i+3, i+2, i+1, i, i+1 \rangle\rangle$,
(c) $\langle\langle i, i+1, i+2, i+1, i, i+1, i+2, i+3 \rangle\rangle$,
(d) $\langle\langle i, i+1, i+2, i+1, i, i+1, i, i+1 \rangle\rangle$,
(e) $\langle\langle i, i+1, i, i+1, i+2, i+3, i+2, i+3 \rangle\rangle$,
(f) $\langle\langle i, i+1, i, i+1, i, i+1, i+2, i+3 \rangle\rangle$,
(g) $\langle\langle i, i+1, i+2, i+3, i, i+3, i+2, i+1 \rangle\rangle$,
(h) $\langle\langle i, i+1, i+2, i+3, i+2, i+3, i+2, i+1 \rangle\rangle$,
(i) $\langle\langle i, i+1, i+2, i+3, i+2, i+1, i+2, i+1 \rangle\rangle$,
(j) $\langle\langle i, i+1, i+2, i+1, i+2, i+1, i+2, i+1 \rangle\rangle$,
(k) $\langle\langle i, i+1, i+2, i+1, i+2, i+1, i, i+1 \rangle\rangle$,
(l) $\langle\langle i, i+1, i, i+1, i, i+1, i, i+1 \rangle\rangle$, and
(m) $\langle\langle i, i+1, i, i+1, i+2, i+1, i+2, i+3 \rangle\rangle$.

Lemma 3.4.9 *Let n be odd and let the order of α be 8 with $\alpha^4 \equiv -1 \pmod{n}$. The following is the list of all type sequences of the non-coiled 8-cycles occurring* *in* $M(\alpha; 4, n)$*. Each type sequence is preceded by a letter corresponding to its block sequence.*

- $n \notin \{17, 41, 73, 97\}$:

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$

- $n = 17, \alpha = 2$:

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$
  (b) $\langle 1, \alpha, -\alpha^2, -\alpha^2, \alpha, 1, 1, 1\rangle$
  (c_1) $\langle 1, \alpha, \alpha, 1, 1, -\alpha, \alpha^2, \alpha^3\rangle$
  (c_2) $\langle 1, \alpha, \alpha, -1, -1, \alpha, \alpha^2, \alpha^3\rangle$

- $n = 41, \alpha = 3$:

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$
  (d) $\langle 1, -\alpha, -\alpha, 1, 1, 1, 1, 1\rangle$
  (e_1) $\langle 1, 1, 1, -\alpha, \alpha^2, \alpha^2, \alpha^2, -\alpha^3\rangle$
  (e_2) $\langle 1, 1, 1, -\alpha, -\alpha^2, -\alpha^2, -\alpha^2, \alpha^3\rangle$

- $n = 73, \alpha = 10$:

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$
  (f_1) $\langle 1, 1, 1, 1, 1, -\alpha, \alpha^2, \alpha^3\rangle$

- $n = 97, \alpha = 33$:

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$
  (f_2) $\langle 1, 1, 1, 1, 1, -\alpha, -\alpha^2, -\alpha^3\rangle$

PROOF. A cycle with a given type sequence occurs in the graph $M(\alpha; 4, n)$ if and only if the corresponding congruence equality holds. For each of the block sequences (a)–(m) we will find all possible non-equivalent type sequences associated with it. To the congruence equation of each of the type sequences we will apply the squaring elimination method from the proof of Lemma 3.4.7 to either confirm the type sequence or prove that it does not occur.

Throughout this proof let $\delta_1, \delta_2, \delta_3 \in \{-1, 1\}$.

The block sequence (a) yields one of the following type sequences:

(a_1) $\langle 1, \delta_1\alpha, \delta_1\alpha, -1, -1, -\delta_1\alpha, -\delta_1\alpha, 1\rangle$,

(a_2) $\langle 1, \delta_1\alpha, \delta_1\alpha, 1, 1, \delta_1\alpha, \delta_1\alpha, 1\rangle$,

(a_3) $\langle 1, \delta_1\alpha, \delta_1\alpha, 1, 1, -\delta_1\alpha, -\delta_1\alpha, 1\rangle$, or

(a_4) $\langle 1, \delta_1\alpha, \delta_1\alpha, -1, -1, \delta_1\alpha, \delta_1\alpha, 1\rangle$.

The type sequences (a_2), (a_3), and (a_4) imply $4 + 4\delta_1\alpha \equiv 0 \pmod{n}$, $4 \equiv 0 \pmod{n}$, and $4\delta_1\alpha \equiv 0 \pmod{n}$, respectively, and each of these congruences is easily seen to yield a contradiction. The congruence equation for (a_1), however, holds for any n and any α. We obtain $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$ and $\langle 1, -\alpha, -\alpha, -1, -1, \alpha, \alpha, 1\rangle$, but these two type sequences are equivalent hence it is enough to make a note of

$$\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle.$$

The block sequence (b) requires one of these two type sequences:

(b_1) $\langle 1, \delta_1\alpha, \delta_2\alpha^2, \delta_2\alpha^2, \delta_1\alpha, 1, 1, 1\rangle$ or

(b_2) $\langle 1, \delta_1\alpha, \delta_2\alpha^2, \delta_2\alpha^2, -\delta_1\alpha, 1, 1, 1\rangle$.

The type (b_1) gives

$$4 + 2\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0 \pmod{n} \tag{3.15}$$

which (after applying the squaring elimination method) implies $n \in \{9, 17\}$. But $\varphi(9) = 6$ is not divisible by 8 so that $n = 17$. Using $\alpha = 2$ (by Lemma 3.4.6 we may pick any order-eight element of Z_n^*) we can check that the equation (3.15) is satisfied only for $\delta_1 = 1$, $\delta_2 = -1$, and this produces the type sequence

$$\langle 1, 2, -2^2, -2^2, 2, 1, 1, 1\rangle.$$

From (b_2) we get $4 + 2\delta_2\alpha^2 \equiv 0 \pmod{n}$, which yields $n = 5$, a contradiction.

The block sequence (c) is associated with one of the following type sequences:

(c_1) $\langle 1, \delta_1\alpha, \delta_1\alpha, 1, 1, -\delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3\rangle$,

(c_2) $\langle 1, \delta_1\alpha, \delta_1\alpha, -1, -1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3\rangle$,

(c_3) $\langle 1, \delta_1\alpha, \delta_1\alpha, -1, -1, -\delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3\rangle$, or

(c_4) $\langle 1, \delta_1\alpha, \delta_1\alpha, 1, 1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3\rangle$.

The equation for (c_1) is

$$3 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n} \tag{3.16}$$

and this implies $n = 17$. Using $\alpha = 2$ we can see that (3.16) can be satisfied only when $\delta_1 = \delta_2 = \delta_3 = 1$ and thus we obtain the type sequence

$$\langle 1, 2, 2, 1, 1, -2, 2^2, 2^3\rangle.$$

The equation for (c_2) is

$$-1 + 3\delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n} \tag{3.17}$$

and again this implies $n = 17$. Using $\alpha = 2$, (3.17) can hold only when $\delta_1 = \delta_2 = \delta_3 = 1$. Thus we get

$$\langle 1, 2, 2, -1, -1, 2, 2^2, 2^3\rangle.$$

The equation for (c_3) is $-1 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. Since the graph has coiled girth 8, it can not be satisfied.

The equation for (c_4) is $3 + 3\delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$ and this implies $n \in \{25, 49\}$, which is impossible since neither $\varphi(25) = 20$ nor $\varphi(49) = 42$ is divisible by 8.

The block sequence (d) is associated with the type sequence

$$\langle 1, \delta_1\alpha, \delta_1\alpha, 1, 1, 1, 1, 1\rangle.$$

The equation is $6 + 2\delta_1\alpha \equiv 0 \pmod{n}$, which implies $n = 41$. Using $\alpha = 3$, $\delta_1 = -1$ is forced and so we have the type sequence

$$\langle 1, -3, -3, 1, 1, 1, 1, 1\rangle.$$

With the block sequence (e) we are looking for the type sequence

$$\langle 1, 1, 1, \delta_1\alpha, \delta_2\alpha^2, \delta_2\alpha^2, \delta_2\alpha^2, \delta_3\alpha^3\rangle,$$

which requires

$$3 + \delta_1\alpha + 3\delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}.$$

By squaring elimination we need $n = 41$. Using $\alpha = 3$, we can check that there are two possibilities: either $\delta_1 = \delta_3 = -1$ and $\delta_2 = 1$, or $\delta_1 = \delta_2 = -1$ and $\delta_3 = 1$. We thus obtain two non-equivalent type sequences,

$$\langle 1, 1, 1, -3, 3^2, 3^2, 3^2, -3^3 \rangle$$

and

$$\langle 1, 1, 1, -3, -3^2, -3^2, -3^2, 3^3 \rangle.$$

The block sequence (f) requires the type sequence

$$\langle 1, 1, 1, 1, 1, \delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3 \rangle$$

and so the equation is

$$5 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}. \tag{3.18}$$

This implies $n \in \{73, 97\}$.

Using $\alpha = 10$ for $n = 73$, (3.18) can hold only when $\delta_1 = -1$ and $\delta_2 = \delta_3 = 1$. We obtain the type sequence

$$\langle 1, 1, 1, 1, 1, -10, 10^2, 10^3 \rangle.$$

For $n = 97$ and $\alpha = 33$, (3.18) can be satisfied only when $\delta_1 = \delta_2 = \delta_3 = -1$ giving the type sequence

$$\langle 1, 1, 1, 1, 1, -33, -33^2, -33^3 \rangle.$$

In the rest of the proof we will show that cycles with block sequences (g)–(m) do not occur.

The block sequence (g) requires an equation of the form

$$2 + 2\varepsilon_1\alpha + 2\varepsilon_2\alpha^2 + 2\varepsilon_3\alpha^3 \equiv 0 \pmod{n}$$

for some $\varepsilon_1, \varepsilon_2 \in \{-1, 0, 1\}$ and $\varepsilon_3 \in \{-1, 1\}$. Dividing this equation by 2, we get the equation (3.13) with $\varepsilon_0 = 1$ and $\varepsilon_3 \in \{-1, 1\}$. It now follows from the proof of Lemma 3.4.7 that this equation can not be satisfied.

The block sequence (h) is associated with one of

$$2 + 2\delta_1\alpha + 4\delta_2\alpha^2 \equiv 0 \pmod{n}$$

and

$$2 + 4\delta_2\alpha^2 \equiv 0 \pmod{n}.$$

The first equation implies $n = 17$, but $\alpha = 2$ does not satisfy any equation of this form. The second equation implies $n = 5$, a contradiction.

The block sequence (i) needs one of the following two equations:

$$2 + 4\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0 \pmod{n}$$

and

$$2 + 2\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0 \pmod{n}.$$

The latter is impossible by the proof of Lemma 3.4.7, and the first one implies $n \in \{3, 9\}$, a contradiction.

The block sequence (j) is associated with

$$2 + 6\delta_1\alpha \equiv 0 \pmod{n},$$

which implies $n = 41$. But using $\alpha = 3$, the equation can not be satisfied.

The block sequence (k) implies

$$4 + 4\delta_1\alpha \equiv 0 \pmod{n},$$

which is easily seen to be impossible to satisfy.

The block sequence (l) requires $8 \equiv 0 \pmod{n}$, clearly impossible.

The block sequence (m) implies

$$3 + 3\delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n},$$

which is the same equation as for (c_4) and hence impossible.

This completes the proof. $\square$

We continue with an analogue of the previous lemma for the case that the order of α is 4.

Lemma 3.4.10 *Let n be odd such that $n \not\equiv 0$ $(mod\ 5)$ and let α have order 4 with $\alpha^2 \not\equiv -1$ $(mod\ n)$. The following is the list of all type sequences of the non-coiled 8-cycles occurring in $M = M(\alpha; 4, n)$. Each type sequence is preceded by a letter corresponding to its block sequence.*

- *M has coiled girth 8 :*

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1 \rangle$

- *M has coiled girth 4 :*

  (a) $\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1 \rangle$

  (c_3) $\langle 1, -\alpha, -\alpha, -1, -1, \alpha, -\alpha^2, -\alpha^3 \rangle$

PROOF. We shall examine the type sequences associated with the block sequences (a)–(m) in a way very similar to that of the proof of Lemma 3.4.9, except that when applying the squaring elimination method we are now using $(\alpha^2)^2 \equiv 1$ (mod n). We also let $\delta_1, \delta_2, \delta_3 \in \{-1, 1\}$ and we label the type sequences as before. Notice that, since $\alpha^2 \not\equiv -1$ (mod n), n is not a prime power.

The case with the block sequence (a) is done in exactly the same way as in the proof of Lemma 3.4.9.

The type sequence (b_1) requires $4 + 2\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0$ (mod n). This implies $-(4\delta_2 - 1)\alpha^2 \equiv 5$ (mod n) and $(4\delta_2 - 1)^2 \equiv 25$ (mod n). Since $9 \equiv 25$ (mod n) is impossible, we must have $\delta_2 = -1$. Hence $5\alpha^2 \equiv 5$ (mod n). Since $\gcd(n, 5) = 1$, this implies $\alpha^2 \equiv 1$ (mod n) which is a contradiction.

From the type sequence (b_2) we get $4 + 2\delta_2\alpha^2 \equiv 0$ (mod n), which yields $n = 3$, a contradiction.

The equation for the type sequence (c_1) is $3 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. This implies $(3\delta_1 - 1)\alpha^2 \equiv \delta_1\delta_3 - 5 \pmod{n}$ and $(3\delta_1 - 1)^2 \equiv (\delta_1\delta_3 - 5)^2 \pmod{n}$. Since none of $4 \equiv 16 \pmod{n}$, $4 \equiv 36 \pmod{n}$, and $16 \equiv 36 \pmod{n}$ can hold, $\delta_1 = -1$ and $\delta_1\delta_3 = 1$. But then $4\alpha^2 \equiv 4 \pmod{n}$, a contradiction.

The equation for the type sequence (c_2) is $-1 + 3\delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. Again, this implies $4\alpha^2 \equiv 4 \pmod{n}$.

The type sequence (c_3) is $\langle 1, \delta_1\alpha, \delta_1\alpha, -1, -1, -\delta_1\alpha, \delta_2\alpha^2, \delta_3\alpha^3\rangle$ and the corresponding equation is $-1 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. This equation can be satisfied if and only if M has coiled girth 4. In that case we may assume by Lemma 3.4.8 that $\delta_1 = \delta_2 = \delta_3 = -1$. Hence M contains 8-cycles with a type sequence

$$\langle 1, -\alpha, -\alpha, -1, -1, \alpha, -\alpha^2, -\alpha^3\rangle.$$

The equation for the type sequence (c_4) is $3 + 3\delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. This implies $(3\delta_2 - 5)\alpha^2 \equiv 3\delta_1\delta_3 - 5 \pmod{n}$ and $(3\delta_2 - 5)^2 \equiv (3\delta_1\delta_3 - 5)^2 \pmod{n}$. Hence either $4 \equiv 64 \pmod{n}$, $2\alpha^2 \equiv 2 \pmod{n}$, or $8\alpha^2 \equiv 8 \pmod{n}$. The first possibility implies that n divides 15, which is impossible, and the other two possibilities contradict the fact that the order of α is 4.

The block sequence (d) is associated with the equation $6 + 2\delta_1\alpha \equiv 0 \pmod{n}$. This implies $n = 5$, a contradiction.

With the block sequence (e), the equation $3 + \delta_1\alpha + 3\delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$ is needed. This implies $\alpha^2 \equiv \pm 1 \pmod{n}$, a contradiction.

The block sequence (f) requires $5 + \delta_1\alpha + \delta_2\alpha^2 + \delta_3\alpha^3 \equiv 0 \pmod{n}$. This implies $n \in \{3, 5, 9, 15, 27, 45\}$ which is a contradiction since each of these numbers is either a prime power or a multiple of 5.

The block sequence (g) yields an equation of the form $1 + \varepsilon_1\alpha + \varepsilon_2\alpha^2 + \varepsilon_3\alpha^3 \equiv 0 \pmod{n}$ for some $\varepsilon_1, \varepsilon_2 \in \{-1, 0, 1\}$ and $\varepsilon_3 \in \{-1, 1\}$. By the proof of Lemma 3.4.8, this equation can not be satisfied to give a type sequence of an 8-cycle.

The block sequence (h) is associated with one of $2 + 2\delta_1\alpha + 4\delta_2\alpha^2 \equiv 0 \pmod{n}$ and $2 + 4\delta_2\alpha^2 \equiv 0 \pmod{n}$. The first equation implies $\alpha^2 \equiv 1 \pmod{n}$ and the second equation implies $n = 3$.

The block sequence (i) needs one of the following two equations: $2 + 4\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0 \pmod{n}$ and $2 + 2\delta_1\alpha + 2\delta_2\alpha^2 \equiv 0 \pmod{n}$. The latter is impossible by the proof of Lemma 3.4.8, and the first one implies $\alpha^2 \equiv 1 \pmod{n}$.

The block sequence (j) is associated with $2 + 6\delta_1\alpha \equiv 0 \pmod{n}$, which implies $n = 5$, impossible.

The equations $4 + 4\delta_1\alpha \equiv 0 \pmod{n}$ and $8 \equiv 0 \pmod{n}$ for the block sequences (k) and (l), respectively, are easily seen to be impossible to satisfy.

The equation for the block sequence (m) is the same as for the type sequence (c_4) and hence impossible.

This covers all cases. □

Definition 3.4.11 The triple (k_1, k_2, k_3) is called the *2-path code* of the graph $M(\alpha; 4, n)$ if every 2-path with the type sequence $\langle 1, 1\rangle$ lies in exactly k_1 8-cycles, every 2-path with the type sequence $\langle \alpha^3, 1\rangle$ lies in exactly k_2 8-cycles, and every 2-path with the type sequence $\langle -\alpha^3, 1\rangle$ lies in exactly k_3 8-cycles in $M(\alpha; 4, n)$.

Similarly, (k_1, k_2, k_3) is called the *2-path code* of a given type sequence of an 8-cycle if every 2-path with the type sequence $\langle 1, 1\rangle$ lies in exactly k_1 8-cycles, every 2-path with the type sequence $\langle \alpha^3, 1\rangle$ lies in exactly k_2 8-cycles, and every 2-path with the type sequence $\langle -\alpha^3, 1\rangle$ lies in exactly k_3 8-cycles with the given type sequence.

Lemma 3.4.12 *Let n be odd, let the order of α be 8 and let $\alpha^4 \equiv -1 \pmod{n}$. If $n \notin \{17, 41, 73, 97\}$, then the 2-path code of $M(\alpha; 4, n)$ is $(2, 5, 5)$. The 2-path code of $M(2; 4, 17)$ is $(8, 12, 12)$, the 2-path code of $M(3; 4, 41)$ is $(13, 12, 7)$, the 2-path code of $M(10; 4, 73)$ is $(6, 8, 6)$, and the 2-path code of $M(33; 4, 97)$ is $(6, 6, 8)$.*

Proof. First notice that it is enough to count the number of 8-cycles for the 2-paths with jump sequences $\langle 1, 1\rangle$, $\langle \alpha^3, 1\rangle$, and $\langle -\alpha^3, 1\rangle$.

By Lemma 3.4.7, a 2-path with a jump sequence $\langle \alpha^3, 1\rangle$ or $\langle -\alpha^3, 1\rangle$ lies in exactly four coiled 8-cycles, and a 2-path with jump sequence $\langle 1, 1\rangle$ does not lie in a coiled 8-cycle.

Thus it remains to consider the non-coiled 8-cycles. By Lemma 3.4.9, the only possible type sequences for a non-coiled 8-cycle are those denoted by (a)–(f_2). For each type sequence, all possible jump sequences are obtained by multiplying each term of the type sequence by α^i, $i = 0, 1, \ldots, 7$. Here, one has to be careful, because two distinct powers of α might give the same jump sequence. (This happens if the sequence has some kind of symmetry.) Once we have found all possible pairwise distinct jump sequences of a given type sequence, we simply count the number of occurrences of the jump sequence of a 2-path. Note that $\langle -1, -1\rangle$, $\langle -1, -\alpha^3\rangle$, and $\langle -1, \alpha^3\rangle$ count as occurrences of $\langle 1, 1\rangle$, $\langle \alpha^3, 1\rangle$, and $\langle -\alpha^3, 1\rangle$, respectively. With jump sequence $\langle 1, 1\rangle$ we have to distinguish between occurrences of $\langle 1, 1\rangle$ with the block sequence $\langle\langle i+1, i, i+1\rangle\rangle$ and those with corresponding block sequence $\langle\langle i, i+1, i\rangle\rangle$. But since the number of occurrences of the subsequences of the form $\langle\langle i+1, i, i+1\rangle\rangle$ in a block sequence of any cycle is the same as the number of occurrences of the subsequences of the form $\langle\langle i, i+1, i\rangle\rangle$, we can limit ourselves to counting the number of occurrences of the jump sequence $\langle 1, 1\rangle$ with corresponding block sequence of the form $\langle\langle i+1, i, i+1\rangle\rangle$.

Following the above method for every type sequence we obtain the following table.

	type sequence	2-path code
(a)	$\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$	$(2, 1, 1)$
(b)	$\langle 1, \alpha, -\alpha^2, -\alpha^2, \alpha, 1, 1, 1\rangle$	$(2, 1, 1)$
(c_1)	$\langle 1, \alpha, \alpha, 1, 1, -\alpha, \alpha^2, \alpha^3\rangle$	$(2, 3, 3)$
(c_2)	$\langle 1, \alpha, \alpha, -1, -1, \alpha, \alpha^2, \alpha^3\rangle$	$(2, 3, 3)$
(d)	$\langle 1, -\alpha, -\alpha, 1, 1, 1, 1, 1\rangle$	$(3, 1, 0)$
(e_1)	$\langle 1, 1, 1, -\alpha, \alpha^2, \alpha^2, \alpha^2, -\alpha^3\rangle$	$(4, 3, 1)$
(e_2)	$\langle 1, 1, 1, -\alpha, -\alpha^2, -\alpha^2, -\alpha^2, \alpha^3\rangle$	$(4, 3, 1)$

	type sequence	2-path code
(f_1)	$\langle 1,1,1,1,1,-\alpha,\alpha^2,\alpha^3\rangle$	$(4,3,1)$
(f_2)	$\langle 1,1,1,1,1,-\alpha,-\alpha^2,-\alpha^3\rangle$	$(4,1,3)$
coiled		$(0,4,4)$

Using Lemma 3.4.9, we now sum up the 2-path codes of the type sequences corresponding to the given value of n to obtain the 2-path code of the graph $M(\alpha;4,n)$. This completes the proof. □

Lemma 3.4.13 *Let n be odd such that $n \not\equiv 0 \pmod 5$ and let α have order 4 with $\alpha^2 \not\equiv -1 \pmod n$. The 2-path code of $M = M(\alpha;4,n)$ is $(4,6,9)$ if M has coiled girth 4, and $(2,5,5)$ if M has coiled girth 8.*

Proof. We use the method described in the proof of the preceding lemma and the information about the 8-cycles from Lemmas 3.4.8 and 3.4.10. The only difference is that, since $-1 \notin \{\alpha^i : i = 0,1,2,3\}$, all possible jump sequences are obtained from a given type sequence by multiplying each term of the type sequence by α^i and $-\alpha^i$, $i = 0,1,2,3$. Again we have to make sure that we count occurrences of the jump sequences $\langle 1,1\rangle$, $\langle \alpha^3,1\rangle$, and $\langle -\alpha^3,1\rangle$ only in distinct jump sequences of the 8-cycles.

If M has coiled girth 8, we obtain the following table.

	type sequence	2-path code
(a)	$\langle 1,\alpha,\alpha,-1,-1,-\alpha,-\alpha,1\rangle$	$(2,1,1)$
coiled		$(0,4,4)$

If M has coiled girth 4, the table is somewhat different.

	type sequence	2-path code
(a)	$\langle 1, \alpha, \alpha, -1, -1, -\alpha, -\alpha, 1\rangle$	$(2, 1, 1)$
(c_3)	$\langle 1, -\alpha, -\alpha, -1, -1, \alpha, -\alpha^2, -\alpha^3\rangle$	$(2, 2, 4)$
coiled		$(0, 3, 4)$

Summing up the 2-path codes of the type sequences of the cycles we obtain the result. □

We now have all the information we need to prove that certain graphs $M(\alpha; 4, n)$ are $\frac{1}{2}$-transitive.

Lemma 3.4.14 *Let n be odd. In addition, either let the order of α be 8 with $\alpha^4 \equiv -1 \pmod n$ or let the order of α be 4 with $\alpha^2 \not\equiv -1 \pmod n$ and $n \not\equiv 0 \pmod 5$. Let (k_1, k_2, k_3) be the 2-path code of the graph $M = M(\alpha; 4, n)$. If $k_2 \neq k_1 \neq k_3$, then M is $\frac{1}{2}$-transitive.*

PROOF. First we show that any automorphism of M that fixes two adjacent vertices is the identity.

Suppose that $\sigma \in \mathrm{Aut}(M)$ fixes the vertices v_0^0 and v_1^1. Then σ fixes the set $\{v_{-1}^1, v_{-\alpha^3}^3, v_{\alpha^3}^3\}$ setwise. Since the 2-paths $v_{-\alpha^3}^3\, v_0^0\, v_1^1$ and $v_{\alpha^3}^3\, v_0^0\, v_1^1$ are contained in k_2 and k_3 8-cycles, respectively, and $v_{-1}^1\, v_0^0\, v_1^1$ is contained in $k_1 \neq k_2, k_3$ 8-cycles, σ must fix v_{-1}^1 as well. Hence σ fixes $\{v_{-2}^0, v_{-1+\alpha}^2, v_{-1-\alpha}^2\}$ setwise. Now, the jump sequence of $v_{-1+\alpha}^2\, v_{-1}^1\, v_0^0$ is $\langle -\alpha, 1\rangle$, which is equivalent to $\langle \alpha^3, 1\rangle$, so that $v_{-1+\alpha}^2\, v_{-1}^1\, v_0^0$ lies in k_2 8-cycles. Similarly, the jump sequence of $v_{-1-\alpha}^2\, v_{-1}^1\, v_0^0$ is $\langle \alpha, 1\rangle$, which is equivalent to $\langle -\alpha^3, 1\rangle$, so that $v_{-1-\alpha}^2\, v_{-1}^1\, v_0^0$ lies is k_3 8-cycles. Since $v_{-2}^1\, v_{-1}^1\, v_0^0$ lies in k_1 8-cycles, v_{-2}^0 must be fixed by σ. And so on.

Since n is odd, $M[V^0, V^1]$ is a $2n$-cycle and so we can see that σ must fix V^0 and V^1 pointwise. Hence σ must be the identity.

Now suppose that M is arc-transitive. Then there exists an automorphism θ that interchanges the vertices v_0^0 and v_1^1. Since θ^2 fixes v_0^0 and v_1^1, θ^2 must be the identity by the above argument. Therefore θ has order 2.

Clearly, θ interchanges $\{v^1_{-1}, v^3_{-\alpha^3}, v^3_{\alpha^3}\}$ and $\{v^0_2, v^2_{1-\alpha}, v^2_{1+\alpha}\}$. Now, the 2-path $v^1_{-1}\, v^0_0\, v^1_1$ cannot be mapped to $v^2_{1-\alpha}\, v^1_1\, v^0_0$ or $v^2_{1+\alpha}\, v^1_1\, v^0_0$ since $k_1 \neq k_2, k_3$, hence θ interchanges v^1_{-1} and v^0_2. Then θ interchanges $\{v^0_{-2}, v^2_{-1+\alpha}, v^2_{-1-\alpha}\}$ and $\{v^1_3, v^3_{2-\alpha^3}, v^3_{2+\alpha^3}\}$, which implies, by an argument similar to the above, that θ interchanges v^0_{-2} and v^1_3. And so on.

Again, since n is odd, $M[V^0, V^1]$ is a $2n$-cycle and so we can see that θ interchanges V^0 and V^1. Consequently, θ interchanges V^2 and V^3. This implies that any coiled 8-cycle is mapped to a coiled 8-cycle.

Let's see how θ acts on the coiled 8-cycles that contain the 2-path $v^3_{\alpha^3}\, v^0_0\, v^1_1$. First we assume that the coiled girth of M is 8. By Lemmas 3.4.7 and 3.4.8, $v^3_{\alpha^3}\, v^0_0\, v^1_1$ is contained in the coiled 8-cycles

$$C_1 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}\, v^0_{1+\alpha+\alpha^2+\alpha^3}\, v^1_{\alpha+\alpha^2+\alpha^3}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0,$$

$$C_2 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha-\alpha^2}\, v^0_{1+\alpha-\alpha^2+\alpha^3}\, v^1_{\alpha-\alpha^2+\alpha^3}\, v^2_{-\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0,$$

$$C_3 = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}\, v^0_{1-\alpha+\alpha^2+\alpha^3}\, v^1_{-\alpha+\alpha^2+\alpha^3}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0, \text{ and}$$

$$C_4 = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha-\alpha^2}\, v^0_{1-\alpha-\alpha^2+\alpha^3}\, v^1_{-\alpha-\alpha^2+\alpha^3}\, v^2_{-\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0.$$

We have seen that $\theta(v^3_{\alpha^3}) \in \{v^2_{1+\alpha}, v^2_{1-\alpha}\}$.

If $\theta(v^3_{\alpha^3}) = v^2_{1+\alpha}$, then $\theta(v^2_{1+\alpha}) = v^3_{\alpha^3}$ since $\theta^2 = 1$. Hence $\theta(C_2)$ contains the 3-path $v^2_{1+\alpha}\, v^1_1\, v^0_0\, v^3_{\alpha^3}$ and so $\theta(C_2) \in \{C_1, C_2\}$.

If $\theta(C_2) = C_2$, then θ interchanges $v^0_{1+\alpha-\alpha^2+\alpha^3}$ and $v^1_{\alpha-\alpha^2+\alpha^3}$. But, since $M[V^0, V^1]$ is a $2n$-cycle, θ reverses exactly two edges on this cycle, that is, $v^0_0\, v^1_1$ and $v^0_1\, v^1_0$. This forces $\alpha - \alpha^2 + \alpha^3 \equiv 0 \pmod{n}$, which contradicts the proofs of Lemmas 3.4.7 and 3.4.8.

If $\theta(C_2) = C_1$, then θ interchanges $v^0_{1+\alpha+\alpha^2+\alpha^3}$ and $v^1_{\alpha-\alpha^2+\alpha^3}$. But the action of θ on V^0 is given by $\theta(v^0_j) = v^1_{-j+1}$ so that $-\alpha - \alpha^2 - \alpha^3 \equiv \alpha - \alpha^2 + \alpha^3 \pmod{n}$ is forced. This implies $\alpha^2 \equiv -1 \pmod{n}$, a contradiction.

Hence $\theta(v^3_{\alpha^3}) = v^2_{1-\alpha}$ so that $\theta(C_3) \in \{C_3, C_4\}$. By an argument similar to the above, $\theta(C_3) = C_3$ forces $-\alpha + \alpha^2 + \alpha^3 \equiv 0 \pmod{n}$, and $\theta(C_3) = C_4$ forces $\alpha - \alpha^2 - \alpha^3 \equiv -\alpha - \alpha^2 + \alpha^3 \pmod{n}$, which are both easily seen to be impossible.

If the coiled girth of M is 4, the only coiled 8-cycles that contain the 2-path $v^3_{\alpha^3}\, v^0_0\, v^1_1$ are C_2, C_3, and C_4. If $\theta(v^3_{\alpha^3}) = v^2_{1+\alpha}$, then $\theta(C_2) = C_2$. If $\theta(v^3_{\alpha^3}) = v^2_{1-\alpha}$, then $\theta(C_2) \in \{C_3, C_4\}$. In both cases, a contradiction is obtained as before.

This proves that $M(\alpha; 4, n)$ can not be arc-transitive. $\square$

Lemma 3.4.15 *The graphs $M(\alpha; 4, 73)$ and $M(\alpha; 4, 97)$ are $\frac{1}{2}$-transitive.*

PROOF. First we show that $M(10; 4, 73)$ is $\frac{1}{2}$-transitive. Suppose not. Then there exists an automorphism θ that interchanges the vertices v^0_0 and v^1_1. Hence θ interchanges $\{v^1_{-1}, v^3_{-\alpha^3}, v^3_{\alpha^3}\}$ and $\{v^0_2, v^2_{1-\alpha}, v^2_{1+\alpha}\}$. By Lemma 3.4.12 the 2-paths $v^1_{-1}\, v^0_0\, v^1_1$, $v^3_{\alpha^3}\, v^0_0\, v^1_1$, $v^0_2\, v^1_1\, v^0_0$, and $v^2_{1+\alpha}\, v^1_1\, v^0_0$ lie in six 8-cycles each, and the 2-paths $v^3_{-\alpha^3}\, v^0_0\, v^1_1$ and $v^2_{1-\alpha}\, v^1_1\, v^0_0$ lie in eight 8-cycles each, and thus θ must interchange $v^3_{-\alpha^3}$ and $v^2_{1-\alpha}$. Repeating the same argument several times we can see that θ fixes the cycle

$$C_1 = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}\, v^0_{1-\alpha+\alpha^2-\alpha^3}\, v^1_{-\alpha+\alpha^2-\alpha^3}\, v^2_{\alpha^2-\alpha^3}\, v^3_{-\alpha^3}\, v^0_0$$

interchanging pairs of its vertices in the obvious way. By Lemmas 3.4.7 and 3.4.9, the 3-path $P = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}$ lies in exactly three 8 cycles; one is C_1 and the other two are

$$C_2 = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}\, v^0_{1-\alpha+\alpha^2+\alpha^3}\, v^1_{-\alpha+\alpha^2+\alpha^3}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0$$

and

$$C_3 = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}\, v^0_{1-\alpha+\alpha^2+\alpha^3}\, v^1_{-3}\, v^0_{-2}\, v^1_{-1}\, v^0_0.$$

By the same lemmas, there are exactly three 8-cycles that contain the 3-path $P' = v^2_{\alpha^2-\alpha^3}\, v^3_{-\alpha^3}\, v^0_0\, v^1_1$; one is C_1 and the other two are

$$C'_2 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}\, v^0_{1+\alpha+\alpha^2-\alpha^3}\, v^1_{\alpha+\alpha^2-\alpha^3}\, v^2_{\alpha^2-\alpha^3}\, v^3_{-\alpha^3}\, v^0_0$$

and

$$C'_3 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha-\alpha^2}\, v^2_{1+\alpha-2\alpha^2}\, v^3_{1+\alpha-3\alpha^2}\, v^2_{\alpha^2-\alpha^3}\, v^3_{-\alpha^3}\, v^0_0.$$

Since θ fixes C_1 and interchanges P and P', it maps $\{C_2, C_3\}$ onto $\{C_2', C_3'\}$. It follows then that $\theta(v^0_{1-\alpha+\alpha^2+\alpha^3}) = v^1_{\alpha+\alpha^2-\alpha^3}$ and $\theta(v^0_{1-\alpha+\alpha^2+\alpha^3}) = v^3_{1+\alpha-3\alpha^2}$ at the same time, an obvious contradiction.

Hence $M(\alpha; 4, 73)$ is $\frac{1}{2}$-transitive.

Similarly we prove that $M(33; 4, 97)$ is $\frac{1}{2}$-transitive. Suppose $M(33; 4, 97)$ is arc-transitive. Then there exists an automorphism θ that interchanges the vertices v^0_0 and v^1_1. From the 2-path code of $M(\alpha; 4, 97)$, it follows that θ fixes the 8-cycle

$$C_1 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}\, v^0_{1+\alpha+\alpha^2+\alpha^3}\, v^1_{\alpha+\alpha^2+\alpha^3}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0$$

by interchanging pairs of its vertices (v^0_0, v^1_1), $(v^2_{1+\alpha}, v^3_{\alpha^3})$, $(v^3_{1+\alpha+\alpha^2}, v^2_{\alpha^2+\alpha^3})$, and $(v^0_{1+\alpha+\alpha^2+\alpha^3}, v^1_{\alpha+\alpha^2+\alpha^3})$. The 3-path $P = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}$ lies in exactly three 8-cycles; one is C_1 and the other two are

$$C_2 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}\, v^0_{1+\alpha+\alpha^2-\alpha^3}\, v^1_{\alpha+\alpha^2-\alpha^3}\, v^2_{\alpha^2-\alpha^3}\, v^3_{-\alpha^3}\, v^0_0$$

and

$$C_3 = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^3_{1+\alpha+\alpha^2}\, v^0_{1+\alpha+\alpha^2+\alpha^3}\, v^3_{-3\alpha^3}\, v^0_{-2\alpha^3}\, v^3_{-\alpha^3}\, v^0_0.$$

The three path $P' = v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0\, v^1_1$ also lies in exactly three 8-cycles; one is C_1 and the other two are

$$C_2' = v^0_0\, v^1_1\, v^2_{1-\alpha}\, v^3_{1-\alpha+\alpha^2}\, v^0_{1-\alpha+\alpha^2+\alpha^3}\, v^1_{-\alpha+\alpha^2+\alpha^3}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0$$

and

$$C_3' = v^0_0\, v^1_1\, v^2_{1+\alpha}\, v^1_{1+2\alpha}\, v^2_{1+3\alpha}\, v^1_{1+4\alpha}\, v^2_{\alpha^2+\alpha^3}\, v^3_{\alpha^3}\, v^0_0.$$

Since θ fixes C_1 and maps P to P', it maps $\{C_2, C_3\}$ onto $\{C_2', C_3'\}$. Hence $\theta(v^0_{1+\alpha+\alpha^2+\alpha^3}) \in \{v^1_{-\alpha+\alpha^2+\alpha^3}, v^1_{1+4\alpha}\}$. But we have seen before that $\theta(v^0_{1+\alpha+\alpha^2+\alpha^3}) = v^1_{\alpha+\alpha^2+\alpha^3}$. Hence either $-\alpha + \alpha^2 + \alpha^3 \equiv \alpha + \alpha^2 + \alpha^3$ or $1 + 4\alpha \equiv \alpha + \alpha^2 + \alpha^3$ (mod n), which implies either $\alpha \equiv 0$ or $136 \equiv 0$ (mod 97), a contradiction.

Hence $M(\alpha; 4, 97)$ is $\frac{1}{2}$-transitive. □

We are now ready for the main result.

Theorem 3.4.16 *If the order of α is* 8 *and $\alpha^4 \equiv -1$ (mod n), the graph $M(\alpha; 4, n)$ is $\frac{1}{2}$-transitive whenever it exists.*

PROOF. If $n \equiv 0 \pmod 4$, then $M(\alpha; 4, n)$ does not exist by Lemma 3.4.1. If n is odd, then $M(\alpha; 4, n)$ is $\frac{1}{2}$-transitive by Lemmas 3.4.12, 3.4.14, and 3.4.15. If $n \equiv 2 \pmod 4$, then, by Lemma 3.4.2, $M(\alpha; 4, n)$ consists of two disjoint copies of $M(\alpha \bmod \frac{n}{2}; 4, \frac{n}{2})$ so that it is $\frac{1}{2}$-transitive by the previous observation. □

Notice that the graph $M(\alpha; 4, n)$ exists for any prime n such that 8 divides $\varphi(n) = n - 1$. By Dirichlet's Theorem 1.0.12 there are infinitely many primes of the form $8k + 1$ so that Theorem 3.4.16 produces an infinite family of $\frac{1}{2}$-transitive graphs of degree 4. The smallest member of the family has 68 vertices.

Theorem 3.4.17 *The graph $M(\alpha; 4, n)$ is $\frac{1}{2}$-transitive if the order of α is* 4 *with $\alpha^2 \not\equiv -1$ (mod n) and n is not a multiple of* 4 *or a multiple of* 5.

PROOF. If n is odd, the result follows from Lemmas 3.4.13 and 3.4.14. If $n \equiv 2 \pmod 4$, $M(\alpha; 4, n)$ consists of two disjoint copies of $M(\alpha \bmod \frac{n}{2}; 4, \frac{n}{2})$, which are $\frac{1}{2}$-transitive. □

Theorem 3.4.17 produces another infinite family of $\frac{1}{2}$-transitive graphs. We can see this as follows. Let $p, q \neq 5$ be distinct primes congruent to 1 modulo 4 (by Dirichlet's theorem there are infinitely many such primes), say $p = 4k + 1$ and $q = 4l + 1$. Let $n = pq$. Then, by Theorem 1.0.11, Z_n^* is isomorphic to the direct product of cyclic groups $\langle b \rangle$ and $\langle c \rangle$ of orders $p - 1$ and $q - 1$, respectively. Since $(b^{2k}c^l)^4 = (c^{2l})^2 = 1$ and $(b^k c^{2l})^4 = (b^{2k})^2 = 1$, $\langle b \rangle \times \langle c \rangle$ contains two elements, $b^{2k}c^l$ and $b^k c^{2l}$, whose squares are distinct elements of order 2. Consequently, there exists $\alpha \in Z_n^*$ of order 4 such that $\alpha^2 \not\equiv -1 \pmod n$. For this α, the graph $M(\alpha; 4, n)$ is $\frac{1}{2}$-transitive by Theorem 3.4.17.

Bibliography

[1] B. Alspach and T. D. Parsons, *A construction for vertex-transitive graphs,* Canad. J. Math. **34** (1982), 307-318.

[2] B. Alspach, D. Marušič and L. Nowitz, *Constructing graphs which are $\frac{1}{2}$-transitive,* J. Austral. Math. Soc. Ser. A, to appear.

[3] E. D. Bolker, *Elementary Number Theory, An Algebraic Approach,* W. A. Benjamin, Inc., New York, 1970.

[4] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications,* North-Holland, New York, 1979.

[5] I. Z. Bouwer, *Vertex and edge-transitive but not 1-transitive graphs,* Canad. Math. Bull. **13** (1970), 231-237.

[6] Y. Cheng and J. Oxley, *On weakly symmetric graphs of order twice a prime,* J. Comb. Theory Ser. B **42** (1987), 196-211.

[7] M. Hall, Jr., *The Theory of Groups,* The Macmillan Company, New York, 1968.

[8] D. F. Holt, *A graph which is edge transitive but not arc transitive,* J. Graph Theory **5** (1981), 201-204.

[9] M. W. Liebeck and J. Saxl, *Primitive permutation groups containing an element of large prime order,* J. London Math. Soc. (2) **31** (1985), 237-249.

[10] D. Marušič, *On vertex-symmetric digraphs,* Discrete Math. **36** (1981), 69-81.

[11] D. Marušič, *Vertex transitive graphs and digraphs of order p^k*, Ann. Discrete Math. **27** (1985), 115-128.

[12] B. D. McKay, *Transitive graphs with fewer than 20 vertices*, Math. Comp. **33** (1979), 1101-1121.

[13] B. D. McKay and G. F. Royle, *Constructing the vertex-transitive graphs of order up to 23*, preprint.

[14] D. Passman, *Permutation Groups*, Benjamin, New York, 1968.

[15] C. E. Praeger and G. F. Royle, *Constructing the vertex-transitive graphs of order 24*, preprint.

[16] W. T. Tutte, *Connectivity in Graphs*, Univ. of Toronto Press, Toronto, 1966.

[17] M.-Y. Xu, *Half-transitive graphs of prime-cube order*, preprint.

[18] X. Yu, *On several symmetry conditions for graphs*, Discrete Math. 102 (1992) 51-59.

[19] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.