Discrete Mathematics 36 (1981) 69–81
North-Holland Publishing Company

ON VERTEX SYMMETRIC DIGRAPHS

Dragan MARUŠIČ
Vojke Šmuc 12, Koper 66000, Yugoslavia (University of Reading, England)

Received 19 July 1979
Revised 18 February 1980, and 25 August 1980

It is proved that if p is a prime, k and $m \leq p$ are positive integers, and Γ is a vertex symmetric digraph of order p^k or mp, then Γ has an automorphism all of whose orbits have cardinality p. Vertex symmetric graphs of order $2p$ such that $2p-1$ is not the square of a composite integer and vertex symmetric digraphs of order p^k are characterised.

1. Introduction

In 1967 Turner [10] characterised vertex symmetric graphs of prime order and gave a necessary and sufficient condition for two vertex symmetric graphs of prime order to be isomorphic. His results were improved by Alspach [1]. Frucht, Graver and Watkins [6] characterised the vertex symmetric generalised Petersen graphs.

In this paper we shall extend these results to other classes of vertex symmetric graphs and digraphs. We shall investigate the properties of vertex symmetric digraphs whose order is either a power of a prime or mp (in this paper p always denotes a prime), where $1 \leq m \leq p$.

Throughout the paper Γ will denote a finite digraph, and G will denote a finite group.

2. Preliminaries

A *digraph* Γ consists of a finite set of vertices $V(\Gamma)$ and a set of edges $E(\Gamma) \subseteq V(\Gamma) \times V(\Gamma)$ which is an irreflexive relation on $V(\Gamma)$. $|V(\Gamma)|$ is called the *order* of Γ. A digraph Γ is a *graph* if $E(\Gamma)$ is a symmetric relation.

Let $u, v \in V(\Gamma)$. If $(u, v) \in E(\Gamma)$, we write $u \to v$. If $u \to v$ and $v \to u$, then we say that u is *adjacent* to v, and that u is a *neighbour* of v, and we write $u \sim v$. By $N(v)$ we denote the set of all neighbours of v. The *complement* of Γ is a digraph Γ^c such that $V(\Gamma^c) = V(\Gamma)$ and

$$E(\Gamma^c) = (V(\Gamma) \times V(\Gamma)) \setminus (I \cup E(\Gamma))$$

where I is the identity relation on $V(\Gamma)$.

If $W, W' \subseteq V(\Gamma)$, then $\Gamma[W]$ will denote the subgraph of Γ induced by W, $E(W, W')$ will denote $E(\Gamma) \cap (W \times W')$, and $\Gamma[W, W']$ will denote the subgraph of Γ with the vertex set $W \cup W'$ and the edge set $E(W, W') \cup E(W', W)$. If $E(W, W') = W \times W'$, then we shall write $W \Gamma W'$.

A digraph Γ is *disconnected* if there exists a non-empty proper subset W of $V(\Gamma)$ such that $E(W, V(\Gamma) \setminus W) \cup E(V(\Gamma) \setminus W, W) = \emptyset$, and is *connected* if it is not disconnected. A digraph Γ is *totally disconnected* if $E(\Gamma) = \emptyset$.

For all group-theoretic definitions not defined here we refer the reader to [12]. Let V be a finite set. The identity permutation on V will always be denoted by id. A permutation $g \neq \mathrm{id}$ on V is called *(m, n)-homogeneous* if it has m orbits of cardinality n and no other orbit. It is called *homogeneous* if it is (m, n)-homogeneous for some m, n. A transitive permutation group on V is *r-imprimitive* if it has at least one non-trivial r-block. If $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ is a complete block system of a transitive permutation group G on V, then $\bar{g}$ will denote the permutation on $\mathcal{B}$ induced by $g \in G$ (that means $\bar{g} : B_i \mapsto g(B_i)$, for each $i \in \{1, 2, \ldots, k\}$). By [12, Proposition 7.2] $\bar{G}$, the set of all $\bar{g}$ $(g \in G)$, is a transitive permutation group on $\mathcal{B}$ and the mapping $(g \to \bar{g})$ is a homomorphism of G onto $\bar{G}$.

Let Γ be a digraph. A permutation f on $V(\Gamma)$ induces a permutation on $V(\Gamma) \times V(\Gamma)$. This induced permutation may also be denoted by f, when no confusion will arise. The *automorphism group* $\mathrm{Aut}\,\Gamma$ of Γ is the group of all permutations f on $V(\Gamma)$ such that $f(E(\Gamma)) = E(\Gamma)$.

A digraph Γ is *vertex symmetric* if $\mathrm{Aut}\,\Gamma$ is transitive. A digraph Γ is a *Cayley digraph* if $\mathrm{Aut}\,\Gamma$ contains a regular subgroup. A digraph Γ is *imprimitive* (*r-imprimitive*) if $\mathrm{Aut}\,\Gamma$ contains an imprimitive (r-imprimitive) subgroup. If $\mathcal{B}$ is a complete non-trivial block system of some imprimitive subgroup of $\mathrm{Aut}\,\Gamma$, then $\Gamma(\mathcal{B})$ will denote a digraph such that $V(\Gamma(\mathcal{B})) = \mathcal{B}$ and $(B, B') \in E(\Gamma(\mathcal{B}))$ if and only if neither $B \Gamma B'$ nor $B \Gamma^c B'$. A digraph Γ is *primitive* if it is vertex symmetric and every transitive subgroup of $\mathrm{Aut}\,\Gamma$ is primitive.

In view of our definitions above, every vertex symmetric digraph is either primitive or imprimitive. Furthermore, every vertex symmetric digraph of prime order is by [12, Theorem 8.3] necessarily primitive. However, there exist primitive digraphs whose order is not a prime, for example the odd graphs O_k (defined in [4]) are primitive for sufficiently large k (oral communication by T. Ito). Another example of primitive digraphs of composite order was pointed out to the author by C. Godsil in a personal correspondence. Namely, for each prime $p \equiv \pm 1$ (mod 16) there exists a primitive graph of order $p(p^2-1)/48$ [4, p. 126] whose automorphism group is primitive, is isomorphic to $\mathrm{PSL}(2, p)$, and has no transitive proper subgroup. On the other hand, since the cartesian product of two vertex symmetric digraphs of order $\geqslant 2$ is imprimitive, it follows that there exists an imprimitive digraph of order n for each composite integer n.

Turner [10] called a graph a p-starred polygon if it has a $(1, p)$-homogeneous automorphism. As an extension of this idea, we shall call a digraph Γ *galactic*

((m, n)-*galactic*) if Aut Γ contains a homogeneous ((m, n)-homogeneous) automorphism. If f is a homogeneous automorphism of Γ, then $[f]$ will denote the subgroup of all automorphisms g of Γ such that $g(X)$ is an orbit of f for every orbit X of f.

A digraph Γ is *uniformly galactic* ((m, n)-*uniformly galactic*) if Aut Γ contains a homogeneous ((m, n)-homogeneous) automorphism f such that $[f]$ is transitive.

Proposition 2.1. *If $m, n \geq 2$, then every (m, n)-uniformly galactic digraph Γ is n-imprimitive.*

Proof. Let f be an (m, n)-homogeneous automorphism of Γ such that $[f]$ is transitive. The set of all orbits of f is a complete n-block system of $[f]$. Therefore Γ is n-imprimitive.

We shall abbreviate "uniformly" to U, "galactic graph" to GG, and "galactic digraph" to GD. Thus, for example, (m, n)-UGD will mean "(m, n)-uniformly galactic digraph".

Proposition 2.2. *Let Γ be a vertex symmetric digraph, G be a transitive subgroup of* Aut Γ, *and p be a prime dividing $|V(\Gamma)|$. Then G contains an element of order p.*

Proof. Clearly, $|V(\Gamma)|$ divides $|G|$ and therefore p divides $|G|$. The Sylow theorems imply that G contains an element of order p.

A straightforward consequence of Proposition 2.2 is:

Corollary 2.3. (Turner [10], Alspach [1]). *Every vertex symmetric digraph of order p is a $(1, p)$-GD (and therefore a $(1, p)$-UGD).*

We propose the following problem:

Problem 2.4. *We have seen that every vertex symmetric digraph of prime order is galactic. Does there exist a vertex symmetric digraph which is not galactic?*

We remark that any Cayley digraph C is galactic because its automorphism group Aut C has a regular subgroup and every non-identity element of this subgroup is homogeneous.

The aim of this paper is to find some other classes of vertex symmetric digraphs which are necessarily galactic. A group-theoretic result [12, Theorem 3.4′] implies that a digraph of order p_k (k is a positive integer) is vertex symmetric if and only if it is (p^{k-1}, p)-UG (Theorem 3.3) thus giving a characterisation of vertex symmetric digraphs of prime power order. Furthermore, we shall prove (Theorem 3.4) that if $1 \leq m \leq p$, then every vertex symmetric digraph of order mp is (m, p)-galactic. In addition we shall prove some further results about galactic graphs. In

Section 5, we shall find a necessary and sufficient condition for two $(2, p)$-galactic graphs to be isomorphic (Theorem 5.4). This may be compared with the result of Turner [10, Theorem 3] which gives a necessary and sufficient condition for two $(1, p)$-galactic graphs to be isomorphic and with the result of Alspach and Sutcliffe [2, Theorem 10] which gives a necessary and sufficient condition for two $(2, p)$-uniformly galactic graphs to be isomorphic. Alspach and Sutcliffe [2] and Toida [11] have independently conjectured that every vertex symmetric graph of order $2p$ is $(2, p)$-UG. We shall prove this to be the case for imprimitive graphs of order $2p$ (Theorem 6.2). This result does not generalise to imprimitive graphs of order mp $(3 \leq m \leq p)$ as we shall see in Section 4. A group-theoretic result shows that primitive graphs of order $2p$ cannot exist unless $p \geq 313$ and $2p-1$ is the square of a composite integer. Thus for all other primes, Theorem 6.2 leads to a characterisation of vertex symmetric graphs of order $2p$; this result may be compared with the characterisation of vertex symmetric graphs of order p obtained by Turner [10].

3. Galactic and vertex symmetric digraphs

Proposition 3.1 [12, Theorem 3.4′]. *Let W be an orbit of a permutation group G. If p^k is the highest power of a prime p dividing $|W|$ and P is a Sylow p-subgroup of G, then every shortest orbit of P in W has cardinality p^k.*

Proposition 3.2. *Let Γ be a vertex symmetric digraph of order p^k, where k is a positive integer, and P by a Sylow p-subgroup of* Aut Γ. *Then $Z(P)$, the centre of P, contains a (p^{k-1}, p)-homogeneous element f such that $P \subseteq [f]$ and $[f]$ is transitive.*

Proof. Since every finite p-group has a non-trivial centre [7, Theorem 4.3.1] we can select an element f of $Z(P)$ of order p. Since $f \neq \text{id}$, there is $v \in V(\Gamma)$ such that $f(v) \neq v$. If $w \in V(\Gamma)$, then $g(v) = w$ for some $g \in P$ (since P is by Proposition 3.1 transitive) and so $f(w) = fg(v) = gf(v) \neq g(v) = w$. Hence f has no fixed vertex and so it is (p^{k-1}, p)-homogeneous. Since $f \in Z(P)$, it follows that $P \subseteq [f]$ and so $[f]$ is transitive.

A straightforward consequence of Proposition 3.2 is

Theorem 3.3. *A digraph of order p^k, where k is a positive integer, is vertex symmetric if and only if it is a (p^{k-1}, p)-UGD.*

Theorem 3.3 can be thought of being a characterisation of vertex symmetric digraphs of prime power order and thus a generalisation of Turner's result [10, Theorem 3]. The situation is not quite so nice in the case of vertex symmetric digraphs of order mp $(1 \leq m \leq p)$. In general we can only prove the following result.

Theorem 3.4. *Every vertex symmetric digraph of order* mp $(1 \leq m \leq p)$ *is an* (m, p)*-GD.*

Proof. Let Γ be a vertex symmetric digraph of order mp and P be a Sylow p-subgroup of Aut Γ. If $m = p$, then Γ is an (m, p)-GD in view of Theorem 3.3. We may therefore assume that $m < p$. The cardinality of each orbit of P divides $|P|$ and so is a power of p, and hence must be either 1 or p since $|V(\Gamma)| < p^2$. However, the shortest orbits of P have cardinality p by Proposition 3.1 with $G = \text{Aut}\,\Gamma$ and $W = V(\Gamma)$. Hence P has m orbits of cardinality p and no other orbit. If $f \in P$ and X is an orbit of P, then the restriction f^X of f on X is either id or is $(1, p)$-homogeneous. Let $\mathcal{I}(f)$ and $\mathcal{H}(f)$ be the sets of orbits X of P for which $f^X = \text{id}$ and f^X is $(1, p)$-homogeneous, respectively. Select $g \in P$ for which $|\mathcal{H}(g)|$ is as large as possible. Suppose if possible that $\mathcal{I}(g) \neq \emptyset$. Select $Y \in \mathcal{I}(g)$. Since Y is an orbit of P, $Y \in \mathcal{H}(h)$ for some $h \in P$. For each $X \in \mathcal{H}(g)$ there is clearly at most one $s \in \{1, 2, \ldots, p-1\}$ such that $(g^X)^s = h^X$. Moreover, $|\mathcal{H}(g)| < m \leq p-1$. Therefore there is $r \in \{1, 2, \ldots, p-1\}$ such that, for each $X \in \mathcal{H}(g)$, $(g^X)^r \neq h^X$. Therefore, for each $X \in \mathcal{H}(g)$, $(g^{-r}h)^X \neq \text{id}$ and so $X \in \mathcal{H}(g^{-r}h)$. Moreover, $g^Y = \text{id}$ and so $(g^{-r}h)^Y = h^Y$ which is $(1, p)$-homogeneous and therefore $Y \in \mathcal{H}(g^{-r}h)$. Hence $\mathcal{H}(g) \cup \{Y\} \subseteq \mathcal{H}(g^{-r}h)$, contradicting the definition of g. This contradiction shows that $\mathcal{I}(g) = \emptyset$ and so g is (m, p)-homogeneous and Γ is an (m, p)-GD. □

It can be seen that the Coxeter graph (of order $4 \cdot 7$) [5], the odd graph O_4 (of order $5 \cdot 7$) and the so called H-graph (of order $6 \cdot 17$) [5] are all primitive and therefore by Proposition 2.1 they cannot be uniformly galactic. Furthermore, not all imprimitive digraphs of order mp $(1 \leq m \leq p)$ are uniformly galactic (as we shall see in the next section). In fact, the relationship between imprimitive and uniformly galactic digraphs of order mp $(1 \leq m \leq p)$ is given in Theorem 3.6 below.

Lemma 3.5. *Let* Γ *be a digraph and* $\mathcal{B}$ *be a complete* p*-block system of a transitive subgroup* G *of* Aut Γ *such that* $\Gamma(\mathcal{B})$ *is connected. If* $g \in \text{Ker}(G \to \bar{G})$ *has order* p *and* g^B *is* $(1, p)$*-homogeneous for some* $B \in \mathcal{B}$, *then* g^B *is* $(1, p)$*-homogeneous for all* $B \in \mathcal{B}$.

Proof. Suppose that there exists $B \in \mathcal{B}$ such that $g^B = \text{id}$. Then there exist $X, Y \in \mathcal{B}$ such that g^X is $(1, p)$-homogeneous and $g^Y = \text{id}$, and either $X \to Y$ or $Y \to X$ or $X \sim Y$ in $\Gamma(\mathcal{B})$. Without loss of generality we may assume that $X \to Y$. Since $\bar{G}$ is transitive on $\mathcal{B}$, there exists $h \in G$ such that $h(X) = Y$. There is an integer n such that $h^n(X) = X$ and $X, h(X), \ldots, h^{n-1}(X)$ are all distinct vertices of $\Gamma(\mathcal{B})$. Since $X \to Y$, it follows that neither $X \Gamma Y$ nor $X \Gamma^c Y$. Therefore there are $v_0 \in X$ and $v_1 \in Y$ such that $v_0 \to v_1$. Since g^X is $(1, p)$-homogeneous and $g^Y = \text{id}$, it follows that $X\Gamma\{v_1\}$. Let $v_n = h^{n-1}(v_1)$. Then $v_n \in X$ and $h^{n-1}(X)\,\Gamma\,\{v_n\}$. Since g^X is $(1, p)$-homogeneous, it follows that $h^{n-1}(X)\,\Gamma\,\{v\}$ for each $v \in X$ and therefore $h^{n-1}(X)\,\Gamma X$. This implies $h^n(X)\,\Gamma\, h(X)$, is equivalent $X \Gamma Y$, contradicting the fact that $X \to Y$ in $\Gamma(\mathscr{B})$. Hence, for each $B \in \mathscr{B}$, g^B is not id and so is $(1, p)$-homogeneous since g has order p.

Theorem 3.6. *Let $2 \leq m \leq p$. A digraph of order mp is p-imprimitive if and only if it is an (m, p)-UGD.*

Proof. In view of Proposition 2.1 we only have to show that a p-imprimitive digraph Γ of order mp is an (m, p)-UGD. Let $\mathscr{B}$ be a complete p-block system of a p-imprimitive subgroup G of $\operatorname{Aut}\Gamma$. Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$ be the components of $\Gamma(\mathscr{B})$ and let $\Phi_j = V(\Gamma_j)$ $(j = 1, 2, \ldots, r)$.

Since G is imprimitive and B is a block of cardinality p there exists $f_j \in G$ such that $f_j(B) = B$ and f_j^B is $(1, p)$-homogeneous. Since $|V(\Gamma)| \leq p^2$ and the order of f_j is the least common multiple of the cardinalities of its orbits, f_j has order kp for some integer k prime to p. Let $g_j = f_j^k$. Then the order of g_j is p and g_j^B is $(1, p)$-homogeneous. Clearly, $\bar{g}_j(\mathscr{B}\setminus\{B\}) = \mathscr{B}\setminus\{B\}$ and since $|\mathscr{B}\setminus\{B\}| = m-1 < p$ and the order of $\bar{g}_j$ divides that of g_j, it follows that $Y = \bar{g}_j(Y) = g_j(Y)$ for each $Y \in \mathscr{B}\setminus\{B\}$. Therefore, $g_j(Y) = Y$ for each $Y \in \Phi_j$. Let U_j be the union of all $Y \in \Phi_j$. It is not hard to see that $\{U_j\colon j = 1, 2, \ldots, r\}$ is a complete block system of G and so the constituent G^{U_j} of G on U_j is transitive for each j. Therefore by Lemma 3.5 with Γ, G, $\mathscr{B}$ replaced by $\Gamma[U_j]$, G^{U_j}, Φ_j, it follows that g_j^Y is $(1, p)$-homogeneous for each $Y \in \Phi_j$.

The permutation g on $V(\Gamma)$ such that $g^{U_j} = g_j^{U_j}$ for each $j \in \{1, 2, \ldots, r\}$ has m orbits of cardinality p, namely the blocks $B \in \mathscr{B}$. It is not difficult to see that g is an automorphism of Γ. Since it fixes every element of $\mathscr{B}$, it follows that $G \leq [g]$ and so $[g]$ is transitive. Therefore Γ is an (m, p)-UGD.

4. The line graph of the Petersen graph

In Section 6 we shall show that every 2-imprimitive graph of order $2p$ is also p-imprimitive, which by Theorem 3.6 implies that every imprimitive graph of order $2p$ is a UGG. Unfortunately this does not generalise to graphs of order mp, where $3 \leq m < p$, since the line graph of the Petersen graph will be shown to be a counterexample (of order 15).

Let $T = \{1, 2, 3, 4, 5\}$. Then the set of vertices of the line graph $L(O_3)$ of the Petersen graph is the set of all 2-sets $\{x, y\}$ where x and y are disjoint 2-subsets of T. Two vertices $\{x, y\}$ and $\{u, v\}$ of $L(O_3)$ are adjacent if and only if $|\{x, y\} \cap \{u, v\}| = 1$. If $i \in T$, then E_i will denote the set $\{\{x, y\} \in V(L(O_3))\colon x \cup y = T \setminus \{i\}\}$.

By [3, Theorem 13.5] and [4, §17A] it follows that a permutation f on $V(L(O_3))$ is an automorphism of $L(O_3)$ if and only if it is induced by some permutation $\bar{f}$ on T.

The proof of the following lemma is left to the reader:

Lemma 4.1. *A permutation on T is $(1,5)$-homogeneous if and only if it induces a $(3,5)$-homogeneous automorphism of $L(O_3)$. A permutation on T has one 3-orbit and two 1-orbits if and only if it induces a $(5,3)$-homogeneous automorphism of $L(O_3)$.*

Proposition 4.2. *$L(O_3)$ is a 3-imprimitive $(3,5)$-GG and $(5,3)$-GG, but is not a UGG.*

Proof. Let $\{x_1, y_1\}$, $\{x_2, y_2\}$ be distinct vertices of $L(O_3)$, and $\bar{f} \in S_T$ be such that $\bar{f}(x_1) = x_2$ and $\bar{f}(y_1) = y_2$. Clearly, f takes $\{x_1, y_1\}$ to $\{x_2, y_2\}$ which proves that $\operatorname{Aut} L(O_3)$ is transitive.

For every $f \in \operatorname{Aut} L(O_3)$, it is clear that $f(E_i) = E_i$ if $\bar{f}(i) = i$ and $f(E_i) \cap E_i = \emptyset$ if $\bar{f}(i) \neq i$. Hence E_i is a block of $\operatorname{Aut} L(O_3)$ and $L(O_3)$ is 3-imprimitive. Furthermore, in view of Lemma 4.1, $L(O_3)$ is a $(3,5)$-GG and a $(5,3)$-GG.

Let f be an arbitrary $(3,5)$-homogeneous automorphism of $L(O_3)$. Then $\bar{f}$ is $(1,5)$-homogeneous by Lemma 4.1. Let $i \in T$, $x = \{i, \bar{f}(i)\}$, $y = \{\bar{f}^2(i), \bar{f}^3(i)\}$, $z = \{\bar{f}^2(i), \bar{f}^4(i)\}$, A be the orbit of f containing $\{x, y\}$, and B be the orbit of f containing $\{x, z\}$. Then $L(O_3)[A]$ is a 5-circuit and $L(O_3)[B]$ is totally disconnected. Therefore $[f]$ is not transitive and $L(O_3)$ is not a $(3,5)$-UGG.

Let f be an arbitrary $(5,3)$-homogeneous automorphism of $L(O_3)$. By Lemma 4.1 there exist distinct $i, j, k \in T$ such that $\bar{f}(i) = i$, $\bar{f}(k) = k$, $\bar{f}^3(j) = j \neq \bar{f}(j)$. Let $\lambda = \{\{i, k\}, \{j, \bar{f}(j)\}\}$, and C be the orbit of f containing λ. Then $L(O_3)[C]$ is a 3-circuit. Furthermore, E_i is an orbit of f and, since $L(O_3)[E_i]$ is totally disconnected, it follows that $L(O_3)$ is not a $(5,3)$-UGG.

5. $(2, p)$-galactic graphs

Let $\mathbb{Z}_p$ be the ring of integers mod p and $\mathbb{Z}_p^*$ be the set of non-zero elements of $\mathbb{Z}_p$. If $a \in \mathbb{Z}_p$ and $S \subseteq \mathbb{Z}_p$, let $aS = \{as: s \in S\}$ and $a + S = \{a + s: s \in S\}$.

Let Γ be a $(1,p)$-GG, and $f \in \operatorname{Aut} \Gamma$ be $(1,p)$-homogeneous. Let $x \in V(\Gamma)$, and $x_i = f^i(x)$ $(i \in \mathbb{Z}_p)$. There exists $S \subseteq \mathbb{Z}_p^*$ such that $x_i \sim x_j$ if and only if $j - i \in S$. We call S the *symbol* of Γ relative to f. Clearly, $S = -S$.

A set $S \subseteq \mathbb{Z}_p^*$ is a *symbol* of Γ if it is the symbol of Γ relative to some $(1,p)$-homogeneous automorphism of Γ. Turner [10, Theorem 3] proved

Proposition 5.1. *Let S and S' be symbols of $(1,p)$-galactic graphs Γ and Γ', respectively. Then Γ' is isomorphic to Γ if and only if $S' = aS$ for some $a \in \mathbb{Z}_p^*$.*

Let Γ be a $(2,p)$-GG, $f \in \operatorname{Aut} \Gamma$ be $(2,p)$-homogeneous, X and Y be the two orbits of f, and S and S' be the symbols of $\Gamma[X]$ and $\Gamma[Y]$ relative to f^X and f^Y, respectively. Let $x \in X$, $y \in Y$, and $x_i = f^i(x)$, $y_i = f^i(y)$ ($i \in \mathbb{Z}_p$). There exists $T \subseteq \mathbb{Z}_p$ such that $x_i \sim y_j$ if and only if $j - i \in T$. We say that the ordered triple (S, S', T) *arises* from the ordered quadruple (Γ, f, x, y) and we write $(\Gamma, f, x, y) \to (S, S', T)$. The notation of this paragraph will be used in the statements and proofs of Lemmas 5.2 and 5.3.

Lemma 5.2. *If $h \in \operatorname{Aut} \Gamma$, $g \in h\langle f \rangle h^{-1}$, $u \in h(X)$, $v \in h(Y)$, then there exist $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_p$ such that $(\Gamma, g, u, v) \to (aS, aS', aT + b)$.*

Proof. There exist $c \in \mathbb{Z}_p^*$, and $d, e \in \mathbb{Z}_p$ such that $g = hf^c h^{-1}$, $u = hf^d(x)$ and $v = hf^e(y)$. Let $a = c^{-1}$ and $b = c^{-1}(d - e)$. Then $(\Gamma, g, u, v) \to (aS, aS', aT + b)$.

Lemma 5.3. *If $p > 2$, $T \notin \{\emptyset, \mathbb{Z}_p\}$ and g is a $(2, p)$-homogeneous automorphism of Γ, then $\langle g \rangle$ is conjugate to $\langle f \rangle$ in $\operatorname{Aut} \Gamma$.*

Proof. Let P be the Sylow p-subgroup of $\operatorname{Aut} \Gamma$ containing f. Then

$$k(X) = X, \qquad k(Y) = Y \quad \text{for every } k \in P \tag{1}$$

because otherwise P would be transitive and so $|V(\Gamma)| = 2p$ would divide $|P|$, which is impossible since $p > 2$. Let $f' \in P$. By (1), $f'(x) = x_i$ for some i. Since $f^* = f'f^{-i} \in P$, each orbit of f^* has cardinality 1 or p and is by (1) a subset of X or Y. Since $f^*(x) = x$, X is not an orbit of f^*. Since $T \notin \{\emptyset, \mathbb{Z}_p\}$, it follows that $N(x) \cap Y$ is not $\emptyset$ or Y and so, since $f^*(x) = x$, Y cannot be an orbit of f^*. Therefore every orbit of f^* has cardinality 1, i.e. $f^* = \mathrm{id}$ and so $f' = f^i \in \langle f \rangle$. Hence $P = \langle f \rangle$. The p-subgroup $\langle g \rangle$ of $\operatorname{Aut} \Gamma$ must be contained in a Sylow p-subgroup H of $\operatorname{Aut} \Gamma$. Since all Sylow p-subgroups of $\operatorname{Aut} \Gamma$ are isomorphic, it follows that $H \cong \langle f \rangle$ and therefore $H = \langle g \rangle$. Since all Sylow p-subgroups of $\operatorname{Aut} \Gamma$ are conjugate in $\operatorname{Aut} \Gamma$, there exists $h \in \operatorname{Aut} \Gamma$ such that $\langle g \rangle = h\langle f \rangle h^{-1}$. This proves Lemma 5.3.

By $[S, S', T]$ we shall denote the isomorphism class of all $(2, p)$-galactic graphs Γ such that $(\Gamma, f, x, y) \to (S, S', T)$ for some $(2, p)$-homogeneous automorphism f of Γ and some pair x, y of vertices of Γ belonging to different orbits of f.

Theorem 5.4. *Let $p > 2$, and $S_i, S_i' \subseteq \mathbb{Z}_p^*$, $T_i \subseteq \mathbb{Z}_p$ for $i = 1, 2$. Then $[S_1, S_1', T_1] = [S_2, S_2', T_2]$ if and only if either*

$$\begin{cases} T_1 = T_2 \in \{\emptyset, \mathbb{Z}_p\} \text{ and there exist } a, a' \in \mathbb{Z}_p^* \\ \text{such that } \{S_2, S_2'\} = \{aS_1, a'S_1'\} \end{cases} \tag{1}$$

or

$$\begin{cases} \text{there exist } a \in \mathbb{Z}_p^*,\ b \in \mathbb{Z}_p \text{ such that either} \\ (S_2, S_2', T_2) \text{ or } (S_2', S_2, -T_2) \text{ equals } (aS_1, aS_1', aT_1 + b). \end{cases} \tag{2}$$

Proof. (I) If the condition (1) is satisfied, then $[S_1, S_1', T_1]=[S_2, S_2', T_2]$ in view of Proposition 5.1. Suppose now that the condition (2) is satisfied. Let $\Gamma\in[S_1, S_1', T_1]$, and $(\Gamma, f, x, y)\to(S_1, S_1', T_1)$. Let $c=a^{-1}$, $g=f^c$ and $x'=f^{bc}(x)$. Then $(\Gamma, g, x', y)\to(aS_1, aS_1', aT_1+b)$ and therefore (S_2, S_2', T_2) arises either from (Γ, g, x', y) or from (Γ, g, y, x'). This implies $[S_1, S_1', T_1]=[S_2, S_2', T_2]$.

(II) Suppose that $[S_1, S_1', T_1]=[S_2, S_2', T_2]$. If $T_1\in\{\emptyset, \mathbb{Z}_p\}$, then clearly $T_2=T_1$ and therefore the condition (1) must be satisfied in view of Proposition 5.1. We may therefore assume that T_1 is a non-empty proper subset of $\mathbb{Z}_p$. Let $\Gamma\in[S_1, S_1', T_1]$, $(\Gamma, f, x, y)\to(S_1, S_1', T_1)$ and $(\Gamma, g, u, v)\to(S_2, S_2', T_2)$. In view of Lemma 5.3 there exists $h\in\operatorname{Aut}\Gamma$ such that $g\in h\langle f\rangle h^{-1}$. By Lemma 5.2 there exist $a\in\mathbb{Z}_p^*$ and $b\in\mathbb{Z}_p$ such that (aS_1, aS_1', aT_1+b) arises either from (Γ, g, u, v) or from (Γ, g, v, u). Since (S_2, S_2', T_2), $(S_2', S_2, -T_2)$ arise from (Γ, g, u, v), (Γ, g, v, u) respectively, it follows that either (S_2, S_2', T_2) or $(S_2', S_2, -T_2)$ equals (aS_1, aS_1', aT_1+b) and therefore the condition (2) is satisfied.

The next theorem is due to Alspach and Sutcliffe [2, Theorem 3] although we state it in our own notation. The proof can be carried out using Lemmas 5.2 and 5.3 and a result of Alspach who explicitly determined the automorphism group of a given $(1, p)$-GD [1, Theorem 2].

Theorem 5.5 (Alspach, Sutcliffe [2]). *A* $(2, p)$-GG $\Gamma\in[S, S', T]$ *is a* $(2, p)$-UGG *if and only if either*

$$T\in\{\emptyset, \mathbb{Z}_p\} \quad \textit{and} \quad S'=aS \quad \textit{for some } a\in\mathbb{Z}_p^* \tag{1}$$

or

$$(S, S', -T)=(aS, aS', aT+b) \quad \textit{for some } a\in\mathbb{Z}_p^*, b\in\mathbb{Z}_p. \tag{2}$$

6. A characterisation of imprimitive graphs of order 2p

Let Γ and Γ' be graphs, and m and n be positive integers. By $\Gamma+\Gamma'$ we shall denote the union of disjoint copies of Γ and Γ', and by $n\Gamma$ the union of n disjoint copies of Γ. By K_n, P_n, $K(m, n)$ we shall denote the complete graph of order n, the path of length n, and the graph $(K_m+K_n)^c$ respectively. If $v\in V(\Gamma)$, then $|\Gamma(v)|$ is called the *valency* of v. Γ is said to be *m-valent* if every vertex of Γ has valency m. In this section an *edge* of Γ will be a 2-set $[u, v]=\{(u, v), (v, u)\}$ such that u and v are adjacent vertices of Γ, and $E(\Gamma)$ will denote the set of edges of Γ. A subset Q of $E(\Gamma)$ is an *edge orbit* of a subgroup G of $\operatorname{Aut}\Gamma$ if it is an orbit of the permutation group on $E(\Gamma)$ induced by G. The subgraph of Γ induced by Q will be denoted by $\Gamma\langle Q\rangle$. If $E(\Gamma)$ is an edge orbit of $\operatorname{Aut}\Gamma$, then Γ will be called *edge symmetric*.

Lemma 6.1. *Let Γ, x, y, x_i, y_i, X, Y, S, S', T have the meaning described after the statement of Proposition* 5.1. *If $p>2$, $S=S'$ and $T=\mathbb{Z}_p^*\setminus S$, then* $\operatorname{Aut}\Gamma$ *is p-imprimitive with a complete block system $\{X, Y\}$.*

Proof. Let $i, r \in \mathbb{Z}_p$. Since $S=-S$, $T=-T$ it follows that

$$|(T+r)\cap S| = |(T-r)\cap S| = |T\cap(S+r)|. \tag{1}$$

Moreover, $x_{i+k}\in N(x_i)\cap N(x_{i+r})$ if and only if $k\in S\cap(S+r)$ and $y_{i+k}\in N(x_i)\cap N(x_{i+r})$ if and only if $k\in T\cap(T+r)$. Therefore, if $r\neq 0$, then

$$\begin{aligned}
&|N(x_i)\cap N(x_{i+r})|\\
&=|S\cap(S+r)|+|T\cap(T+r)|\\
&=|S\cap(\mathbb{Z}_p^*+r)|-|S\cap(T+r)|+|T\cap(\mathbb{Z}_p^*+r)|-|T\cap(S+r)|\\
&=|\mathbb{Z}_p^*\cap(\mathbb{Z}_p^*+r)|-2\,|T\cap(S+r)|=p-2-2\,|T\cap(S+r)|
\end{aligned}$$

and so $|N(x_i)\cap N(x_{i+r})|$ is odd for every two distinct vertices $x_i, x_{i+r}\in X$.

Moreover, (since $T=-T$) $x_{i+k}\in N(y_i)\cap N(x_{i+r})$ if and only if $k\in(S-r)\cap T$ and $y_{i+k}\in N(y_i)\cap N(x_{i+r})$ if and only if $k\in S\cap(T+r)$. Therefore $|N(y_i)\cap N(x_{i+r})| = |(S+r)\cap T|+|S\cap(T+r)|$, which is even by (1). Hence $|N(y_i)\cap N(x_{i+r})|$ is even for every two vertices $y_i\in Y$, $x_{i+r}\in X$.

If X, Y are not blocks of $\operatorname{Aut}\Gamma$, then there exist $g\in\operatorname{Aut}\Gamma$, $y_d\in Y$ and $x_a, x_b, x_c\in X$ such that $g(x_a)=x_b$, $g(x_c)=y_d$, which implies that $|N(x_a)\cap N(x_c)| = |N(x_b)\cap N(y_d)|$, and this is impossible since $|N(x_a)\cap N(x_c)|$ is odd and $|N(x_b)\cap N(y_d)|$ is even.

Theorem 6.2. *A graph of order $2p$ is imprimitive if and only if it is a $(2, p)$-UGG.*

Proof. In view of Theorem 3.6 we only have to prove that a 2-imprimitive graph Γ of order $2p$, where $p>2$, is a $(2, p)$-UGG (and thus also p-imprimitive). Let G be a 2-imprimitive subgroup of $\operatorname{Aut}\Gamma$. It is easily seen that G has a $(2, p)$-homogeneous element f. (In fact every element of G of order p is $(2, p)$-homogeneous.) Let X and Y be the orbits of f. Then there exist $x\in X$ and $y\in Y$ such that $\{x, y\}$ is a block of G. Let $(\Gamma, f, x, y)\to(S, S', T)$, and $x_i=f^i(x)$, $y_i=f^i(y)$, $B_i=\{x_i, y_i\}$ $(i\in\mathbb{Z}_p)$. Then $\mathcal{B}=\{B_i : i\in\mathbb{Z}_p\}$ is a complete 2-block system of G. With the notation of Section 2 we shall distinguish two different cases.

Case 1: $\operatorname{Ker}(G\to\bar{G})$ *is non-trivial.*

To prove that Γ is a $(2, p)$-UGG it suffices to show that $[f]$ is transitive. If $\Gamma(\mathcal{B})$ is connected, then (by Lemma 3.5) $\operatorname{Ker}(G\to\bar{G})$ contains a $(p, 2)$-homogeneous element which clearly belongs to $[f]$ and thus $[f]$ is transitive. If $\Gamma(\mathcal{B})$ is not connected, then it must be totally disconnected (since it is vertex symmetric and of order p). Therefore the permutation on $V(\Gamma)$ which interchanges x_i and y_i, for every $i\in\mathbb{Z}_p$, belongs to $[f]$ and so $[f]$ is transitive.

Case 2: $\operatorname{Ker}(G\to\bar{G})$ *is trivial.*

Suppose first that $\bar{G}$ is solvable. Since $|\bar{G}|=|G|\geq 2p$, $\bar{G}$ cannot be regular and so it is by [12, Theorem 11.6] a Frobenius group. By [12, Theorem 5.1] the elements of $\bar{G}$ of degree p together with id form a regular normal subgroup $\bar{H}$ of $\bar{G}$. Since $\bar{H}$ is regular, $|\bar{H}|=p$ and therefore $\bar{H}=\langle\bar{f}\rangle$. Hence $\langle\bar{f}\rangle$ is normal in $\bar{G}$ and therefore $\langle f\rangle$ is normal in G. Hence $G\subseteq[f]$ and therefore $[f]$ is transitive, i.e. Γ is a $(2, p)$-UGG.

If $\bar{G}$ is nonsolvable, then by [12, Theorem 11.7] it is 2-transitive on $\mathcal{B}$. Therefore the subgraphs $B(i, j)=\Gamma[B_i, B_j]$, $i\neq j$ are all isomorphic bipartite graphs. Consider any two distinct $i, j\in\mathbb{Z}_p$. Since $\bar{G}$ is 2-transitive, there is an element of G which interchanges B_i and B_j and therefore $B(i, j)\not\cong K(1,2)+K_1$. Furthermore, $B(i, j)$ also cannot be isomorphic to $K(2,2)$ or $2K_2$ or K_4^c because in all these cases the permutation on $V(\Gamma)$ which interchanges x_i and y_i, for every $i\in\mathbb{Z}_p$, would be a non-identity element of $\mathrm{Ker}(G\to\bar{G})$. Therefore $B(i, j)$ is isomorphic either to K_2+2K_1 or to P_4. Suppose that $B(i, j)\cong P_4$, and $m, k\in\mathbb{Z}_p$ are distinct. Since $\bar{G}$ is 2-transitive, it follows that each end-edge of the path $B(i, j)$ can be mapped by an element of G to each end-edge of the path $B(m, k)$, and cannot be mapped by an element of G to the central edge of the path $B(m, k)$. This means that there exists an edge orbit Q of G such that $\Gamma\langle Q\rangle\cap B(i, j)\cong 2K_2$ for any two distinct $i, j\in\mathbb{Z}_p$. Therefore there exists $\tilde{S}\subseteq\mathbb{Z}_p^*$ such that $\Gamma\langle Q\rangle\in[\tilde{S}, \tilde{S}, \mathbb{Z}_p^*\setminus\tilde{S}]$. By Lemma 6.1, $\mathrm{Aut}\,\Gamma\langle Q\rangle$ is p-imprimitive. Since Q is an edge orbit of G, it follows that $G\subseteq\mathrm{Aut}\,\Gamma\langle Q\rangle$ and therefore G is p-imprimitive. By Theorem 3.6, Γ is a $(2, p)$-UGG. If $B(i, j)\cong K_2+2K_1$, then a similar argument shows that Γ^c is a $(2, p)$-UGG and therefore Γ is a $(2, p)$-UGG.

Remark 6.3. Toida [11] has independently proved that a 2-imprimitive graph Γ of order $2p$ with 2 blocks B_i $(i\in\mathbb{Z}_p)$ is a $(2, p)$-UGG unless the graphs $B(i, j)$, $i\neq j$, are all isomorphic to P_4 or to K_2+2K_1.

Combining Theorems 5.5 and 6.2 we obtain:

Theorem 6.4. *A graph Γ of order $2p$ is imprimitive if and only if there exist $S\subseteq\mathbb{Z}_p^*$, $T\subseteq\mathbb{Z}_p$, $a\in\mathbb{Z}_p^*$, $b\in\mathbb{Z}_p$ such that $\Gamma\in[S, aS, T]$ and either*

(1) *$T\in\{\emptyset, \mathbb{Z}_p\}$ or*

(2) *$a^2S=S$ and $aT+b=-T$.*

If G is a permutation group on V and $v\in V$, then G_v will denote the subgroup of all permutations $g\in G$ such that $g(v)=v$.

Combining the results of Wielandt [12, Theorem 31.2], Feit (umpublished, see [9, p. 56]), Wielandt (unpublished, see [9, p. 56]) and Scott [9, Theorem 1] we obtain:

Theorem 6.5. *Let $|V|=2p$, $v\in V$ and G be a primitive but not 2-transitive permutation group on V. Then $2p=m^2=1$ for some integer m and either m is not prime* *and* $p \geq 313$ *or* $p = 5$. *Furthermore,* C_v *has orbits of cardinalities* $1, \frac{1}{2}m(m-1), \frac{1}{2}m(m+1)$.

Corollary 6.6. *If* Γ *is a primitive graph of order* $2p$, *then* $p \geq 313$, $2p = m^2+1$ *for some composite integer* m, Γ *is either* $\frac{1}{2}m(m-1)$*-valent or* $\frac{1}{2}m(m+1)$*-valent, and both* Γ *and* Γ^c *are edge symmetric.*

Proof. Since Γ is primitive, it is clearly not isomorphic to K_{2p} or K_{2p}^c and so there exist $[u_1, u_2] \in E(\Gamma)$, $[u_3, u_4] \in E(\Gamma^c)$. Since Γ has no automorphism which maps u_1, u_2 into u_3, u_4 respectively, $\operatorname{Aut}\Gamma$ is not 2-transitive. By Theorem 6.5, $2p = m^2+1$ for some integer m. If $v \in V(\Gamma)$, then $(\operatorname{Aut}\Gamma)_v$ has by Theorem 6.5 three orbits of cardinalities 1, $\frac{1}{2}m(m-1)$, $\frac{1}{2}m(m+1)$ and since an element of $(\operatorname{Aut}\Gamma)_v$ cannot map a vertex adjacent to v to a vertex not adjacent to v or vice versa, it follows that the orbits of $(\operatorname{Aut}\Gamma)_v$ are $\{v\}$, $N(v)$, $V(\Gamma)\setminus(N(v)\cup\{v\})$. Thus Γ is either $\frac{1}{2}m(m-1)$-valent or $\frac{1}{2}m(m+1)$-valent. If $p=5$, then Γ is either 3-valent or 6-valent. If Γ is 3-valent, then, by Theorems 3.4 and 5.4, either $\Gamma \in [\{1,-1\}, \{1,-1\}, \{0\}]$ or $\Gamma \in [\{1,-1\}, \{2,-2\}, \{0\}]$ or $\Gamma \in [\emptyset, \emptyset, T]$ for some subset T of $\mathbb{Z}_5$ of cardinality 3. By Theorem 5.5, Γ is a $(2,5)$-UGG and so by Theorem 6.2 is not primitive. If Γ is 6-valent, then Γ^c is 3-valent and the argument above shows that Γ^c is not primitive and thus Γ is not primitive. Therefore $p \neq 5$ and by Theorem 6.5, $p \geq 313$ and m is a composite integer.

Consider any two edges $[x, y]$, $[z, w]$ of Γ. Since Γ is vertex symmetric, there exists $f \in \operatorname{Aut}\Gamma$ such that $f(x) = z$. Clearly $f(y) \in N(z)$. Since $N(z)$ is an orbit of $(\operatorname{Aut}\Gamma)_z$, it follows that $g(f(y)) = w$ for some $g \in (\operatorname{Aut}\Gamma)_z$. Then gf maps $[x, y]$ into $[z, w]$. This proves that Γ is edge symmetric. A similar argument shows that Γ^c is edge symmetric.

For integers n and r with $2 \leq 2r < n$, the generalised Petersen graph $G(n, r)$ [6] is defined by

$$V(G(n,r)) = \{x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{n-1}\}$$

and

$$\begin{aligned} E(G(n,r)) = &\{[x_i, x_{i+1}]: i = 0, 1, \ldots, n-1\} \\ &\cup \{[y_i, y_{i+r}]: i = 0, 1, \ldots, n-1\} \\ &\cup \{[x_i, y_i]: i = 0, 1, \ldots, n-1\} \end{aligned}$$

where the addition is taken mod n. If n is a prime p, then by Theorem 5.4, $G(p, r) \in [S, S', T]$ if and only if $S = \{s, -s\}$, $S' = \{rs, -rs\}$, $T = \{t\}$ for some $s \in \mathbb{Z}_p^*$, $t \in \mathbb{Z}_p$. From this and the fact that (by Corollary 6.6) no $G(p, r)$ is primitive we can deduce by Theorem 6.4 that $G(p, r)$ is vertex symmetric if and only if $r^2 \equiv \pm 1 \pmod p$. Thus the special case in which n is prime of the result of Frucht, Graver and Watkins [6, §1, p. 212], is also a special case of Theorem 6.4.

Combining Theorem 6.4 and Corollary 6.6 we obtain:

Theorem 6.7. *Suppose that either $p<313$ or $2p-1$ is not the square of a composite integer. Then a graph Γ of order $2p$ is vertex symmetric if and only if there exist $S\subseteq \mathbb{Z}_p^*$, $T\subseteq \mathbb{Z}_p$, $a\in \mathbb{Z}_p^*$, $b\in \mathbb{Z}_p$ such that $\Gamma\in[S, aS, T]$ and either*

(1) $T\in\{\emptyset, Z_p\}$ *or*

(2) $a^2S=S$, $aT+b=-T$.

Conjecture 6.8. The only two graphs of order $2p$ with a primitive automorphism group that are known to the author, are O_3 and O_3^c, but they are both imprimitive. This makes us believe that every vertex symmetric graph of order $2p$ is imprimitive. If this is so, the hypothesis that either $p<313$ or $2p-1$ is not the square of a composite integer can be omitted from Theorem 6.7.

Acknowledgement

The author wishes to thank his supervisor Prof. C. St. J. A. Nash-Williams for his guidance and very conscientious reading of the manuscript.

References

[1] B. Alspach, Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, J. Combinatorial Theory 15, (B) (1973) 12–17.
[2] B. Alspach R.J. Sutcliffe, Vertex-transitive graphs of order 2p, Annals N.Y. Acad. Sci. 319 (1979) 18–27.
[3] M. Behzad and G. Chartrand, Introduction to the Theory of Graphs (Allyn and Bacon, Boston, 1971).
[4] N.L. Biggs, Algebraic Graph Theory (Cambridge Univ. Press. 1974).
[5] N.L. Biggs, Three remarkable graphs, Canad. J. Math. 25 (1973) 397–411.
[6] R. Frucht, J.E. Graver and M.E. Watkins, The groups of the generalised Petersen graphs, Proc. Cambridge Philos. Soc. 70 (1971) 211–218.
[7] M. Hall jr., The Theory of Groups (MacMillan, New York, 1959).
[8] F. Harary, Graph Theory (Addison-Wesley, Reading, MA, 1969).
[9] L.L. Scott, Uniprimitive permutation groups, in: Brauer and Sah, eds., Theory of Finite Groups (Benjamin, New York, 1969) 55–61.
[10] J. Turner, Point-symmetric graphs with a prime number of points, J. Combinatorial Theory 3 (1967) 136–145.
[11] S. Toida, Graphs with symmetrics, submitted for publication.
[12] H. Wielandt, Finite Permutation Groups (Academic Press, New York, 1964).