Some Connections Between the Minimal Polynomial and the Automorphism Group of a Graph*

by

Giovanni Criscuolo
Abbe Mowshowitz

Chung-Mo Kwok
Roberto Tortora

Technical Report 77-18

November 1977

Department of Computer Science
The University of British Columbia
Vancouver, British Columbia V6T 1W5

Abstract

The relationship between the spectrum and the automorphism group of a graph is probed with the aid of the theory of finite group representations. Three related topics are explored: 1) graphs with non-derogatory adjacency matrix, 2) point-symmetric graphs, and 3) an algorithm for constructing the automorphism group of a prime, point-symmetric graph. First, we give an upper bound on the order of the automorphism group of a graph with non-derogatory adjacency matrix; and show, in a special case, that the degree of each irreducible factor of the minimal polynomial has a natural interpretation in terms of the automorphism group. Second, we prove that the degree of the minimal polynomial of a point-symmetric graph is bounded above by the number of orbits of the stabilizer of any given element. For point-symmetric graphs with a prime number of points, we exhibit a formula linking the degree of the minimal polynomial with the order of the group. Finally, we give a simple algorithm for constructing the automorphism group of a point-symmetric graph with a prime number of points.

Giovanni Criscuolo
Istituto di Fisica
Teorica
Univ. of Naples
Naples, Italy

Chung-Mo Kwok
Dept. of Mathematics
Univ. of B. C.
Vancouver, Canada

Abbe Mowshowitz
Dept. of Computer
Science
Univ. of B. C.
Vancouver, Canada

Roberto Tortora
Istituto di Matemati
Univ. of Naples
Naples, Italy

* The research reported here was supported in part by Grant #67-7328 from the National Research Council of Canada; and by "Consiglio Nazionale delle Ricerech",

The relationship between the spectrum and the automorphism group of a graph is a fertile area for enlisting the aid of algebraic methods in the study of graphs. We have found the theory of finite group representations to be especially useful in this area. By exploiting this powerful algebraic theory as a unifying instrument, we obtain known results (see for example [3], [7], [8], [9]) in a general setting, and also derive some new results.

We explore three related topics: 1) graphs with non-derogatory adjacency matrix, 2) point-symmetric graphs, and 3) an algorithm for constructing the automorphism group of a prime, point-symmetric graph. In Section 1, we give an upper bound on the order of the automorphism group of a graph with non-derogatory adjacency matrix. In addition, for a special case, we show that the degree of each irreducible factor of the minimal polynomial over the rationals has a natural interpretation in terms of the automorphism group. In Section 2 we prove that the degree of the minimal polynomial of a point-symmetric graph is bounded above by the number of orbits of the stabilizer of any given element. For point-symmetric graphs with a prime number of points, we exhibit a formula linking the degree of the minimal polynomial with the order of the group. In the concluding section, we give a simple algorithm for constructing the automorphism group of a point-symmetric graph with a prime number of points.

The graph-theoretic terminology used in this paper is largely that of Harary [5]. The points and line of a graph G are denoted by V(G) and E(G), respectively. We denote the automorphism group of G by $\Gamma(G)$, the adjacency matrix by A(G), and the minimal polynomial of A(G) (or simply the minimal polynomial of G) by $\mu_G(x)$. A matrix is non-derogatory if its minimal and characteristic polynomials are identical.

1. Graphs with non-derogatory adjacency matrix

Let G be a graph with n points. The set $\Gamma^* = \{P(\gamma) | \gamma\varepsilon\Gamma(G)\}$ is a faithful representation of the automorphism group of G. It is well known (see, for example, [6]) that Γ^* is completely reducible on the complex field. Therefore, for each $\gamma\varepsilon\Gamma(G)$

$$P'(\gamma) = \begin{vmatrix} D_1(\gamma) & & & & & & \\ & \ddots & & & & & \\ & & D_1(\gamma) & & & & \\ & & & \ddots & & & \\ & & & & D_r(\gamma) & & \\ & & & & & \ddots & \\ & & & & & & D_r(\gamma) \end{vmatrix}$$

where $P'(\gamma) = UP(\gamma)U^{-1}$ for a fixed unitary matrix U, and each set $\{D_i(\gamma) | 1\leq i\leq r\}$ is an irreducible representation of $\Gamma(G)$ of dimension m_i.

Clearly, the following relation holds:

$$\sum_{r=1}^{r} e_i m_i = n$$

Since the adjacency matrix A(G) commutes with all elements of Γ^*, it is natural to consider the algebra Δ of all matrices commuting with every element of Γ^*. A matrix B is in Δ iff UBU^{-1} commutes with matrices $P'(\gamma)$ for all $\gamma\varepsilon\Gamma(G)$; moreover (see [2]),

$$UBU^{-1} = \mathrm{diag}[B_{e_1}\times I_{m_1},\ldots,B_{e_r}\times I_{m_r}] \tag{1}$$

where B_{e_i} is a matrix of order e_i and $\times$ denotes the Kronecker product. Thus, the number of distinct eigenvalues of any B in Δ is less than or equal to $\sum_{r=1}^{r} e_i$. Since $A(G)\varepsilon\Delta$ is symmetric, the number of distinct eigenvalues of $A(G)$ over the complex field is also the degree of its minimal polynomial. We have therefore proved the following.

Theorem 1. Let G, A(G), and $e_i (1\leq i\leq r)$ be defined as above. Then

$$\deg \mu_G \leq \sum_{i=1}^{r} e_i .$$

Corollary 1.1. Let G be a point-symmetric graph with $n>2$ points. Then A(G) is derogatory.

Proof. If A(G) is non-derogatory, we have

$$n = \deg \mu_G \leq \sum_{i=1}^{r} e_i \leq \sum_{i=1}^{r} m_i e_i = n$$

which implies $m_i=1$ for each $i(1\leq i\leq r)$. That is to say, Γ^* contains n invariant subspaces of dimension 1. But for $n>2$ this implies that $\Gamma(G)$ is not transitive, because for each transitive group Γ the faithful representation $\Gamma^* = \{P(\gamma)|\gamma\varepsilon\Gamma\}$ must contain exactly one one-dimensional invariant subspace ([13], Thm. 29.1).

The previous Corollary is also a consequence of a theorem of Petersdorf and Sachs [9]. The following is a result due independently to Petersdorf and Sachs [9] and to Mowshowitz [7].

Corollary 1.2. If A(G) is non-derogatory, $\Gamma(G)$ is elementary abelian.

Proof. If indeed $m_i=1$ for each $1\leq i\leq r$, then each $P'(\gamma)$ is a diagonal matrix. This implies (see [13]) that $P(\gamma)$ is symmetric. Hence, $\gamma^2=1$ for each $\gamma\varepsilon\Gamma(G)$. Since the adjacency matrix of a graph is summetric over the complex field and *a fortiori* over the integers, its minimal polynomial is a product of distinct irreducible factors. Using this property some information can be obtained about $|\Gamma G)|$

when $A(G)$ is non-derogatory.

Theorem 2. Let G be a graph whose adjacency matrix $A(G)$ is non-derogatory over the complex field, and such that its minimal polynomial μ_G over the integers splits into k irreducible factors. Then $|\Gamma(G)| \le 2^{k-1}$.

Proof. Suppose G has n points and $\mu_G(x) = \prod_{i-1}^{k} \mu_i(x)$ where $\mu_i(x)$ is irreducible of degree n_i $(1 \le i \le k)$ over the rationals. Then A is similar over the rationals to the matrix $\hat{A} = \mathrm{diag}[A_1, \ldots, A_k]$, where A_i is the companion matrix of $\mu_i(x)$. Since A is non-derogatory, every matrix commuting with A is a polynomial in A (see [11]). In particular, any permutation matrix $P(\gamma)$, $\gamma \varepsilon \Gamma(G)$, is a polynomial in A, for a permutation γ is an automorphism of G iff $P(\gamma)$ commutes with A.

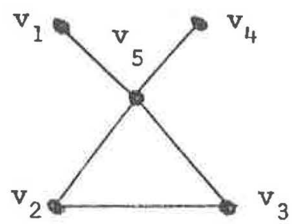
Now let U be the non-singular matrix satisfying $A = U\hat{A}U^{-1}$, and let $\gamma \varepsilon \Gamma(G)$. Then $P(\gamma) = f(A) = UF(\hat{A})U^{-1}$ for some polynomial $f(x)$ over the rationals A, so that $P(\gamma)$ is similar to $f(\hat{A}) = \mathrm{diag}[B_1, B_2, \ldots, B_k]$ where $B_i = f(A_i)$, $1 \le i \le k$. The assumption that A is non-derogatory guarantees (by Corollary 1.2) that $P^2(\gamma) = I_n$. Hence, $B_i^2 = I_{n_i}$ for $1 \le i \le k$. Since A_i has minimal polynomial $\mu_i(x)$ which is irreducible, $Q[A_i]$ is a field (isomorphic to $Q[x]/\mu_i(x)$); and since the only solutions of x^2-1 in $Q[A_i]$ are I_{n_i} and $-I_{n_i}$, $B_i \varepsilon \{I_{n_i}, -I_{n_i}\}$. Thus for any $\gamma \varepsilon \Gamma(G)$, $P(\gamma) = U\mathrm{diag}[B_1, \ldots, B_k]U^{-1}$ where each $B_i \varepsilon \{I_{n_i}, -I_{n_i}\}$. Therefore, the order of $\Gamma(G)$ is less than or equal to 2^k. But the matrix $\mathrm{diag}[-I_n, \ldots, -I_{n_k}]$ cannot be similar to a permutation matrix, because its trace is negative. Moreover, the order of $\Gamma(G)$ must be a power of 2 since $\Gamma(G)$ is elementary abelian. Thus $|\Gamma(G)| \le 2^{k-1}$, as required.

We can analyze two distinct cases when the hypotheses of the theorem are satisfied:

A. $|\Gamma(G)| = 2^{k-1}$

B. $|\Gamma(G)| = 2^m$, where $m \le k-2$

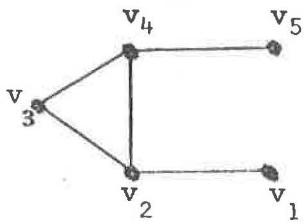
Figure 1 exhibits two 5-point graphs with non-derogatory adjacency matrix which illustrate the two cases.

G: 

$\mu_G(x) = (x^3 - x^2 - 4x + 2)(x + 1)x$

$\Gamma(G) = \{e, (v_1v_4), (v_2v_3), (v_1v_4)(v_2v_3)\}$

$k = 3;\ |\Gamma(G)| = 4 = 2^{k-1}$

H: 

$\mu_H(x) = (x^2 + x - 1)(x^2 - x - 3)x$

$\Gamma(H) = \{e, (v_1v_5)(v_2v_4)\}$

$k = 3;\quad |\Gamma(H)| = 2 < 2^{k-1} = 4$

Figure 1

The following theorem yields a result by Mowshowitz [8] as a special case.

Theorem 3. Let G be a graph whose characteristic polynomial is a product, over the integers, of k distinct irreducible factors. If G is such that case A obtains, then each orbit of $\Gamma(G)$ has cardinality not greater than two.

Proof. If $k = 1$, $\Gamma(G)$ consists of the identity alone, and the theorem follows trivially; if $k = 2$ and $|\Gamma(G)| = 2$, the result is also obvious. So, suppose $k \geq 3$ and $|\Gamma(G)| = 2^{k-1}$. According to Theorem 2, there exists a matrix U such that for each $\gamma \in \Gamma(G)$, $P(\gamma) = U\,\mathrm{diag}[B_1, \ldots, B_k]U^{-1}$, where each B_i is either I_{n_i} or $-I_{n_i}$. If $B_i' = -B_i$ for $1 \leq i \leq k$, then

$$U\,\mathrm{diag}[B_1', \ldots, B_k']U^{-1} = -U\,\mathrm{diag}[B_1, \ldots, B_k] \text{ and}$$

only one of the two matrices can be a permutation matrix. By hypothesis $|\Gamma(G)| = 2^{k-1}$; hence, one and only one of each pair $\mathrm{diag}[B_1, \ldots, B_k]$ and $\mathrm{diag}[-B_1, \ldots, -B_k]$ is similar to an element of $\Gamma^*(G)$. It follows that if any element of the form $\mathrm{diag}[-I_{n_1}, B_2, \ldots, B_k]$ is similar to some element of $\Gamma^*(G)$, then $B = U\mathrm{diag}[-I_{n_1}, I_{n_2}, \ldots, I_{n_k}]U^{-1}$ must be in $\Gamma^*(G)$. Moreover, both

$$\mathrm{diag}[I_{n_1}, I_{n_2}, I_{n_3}, -I_{n_4}, \ldots, I_{n_{2i+1}}, -I_{n_{2i+2}}, \ldots]$$
and
$$\mathrm{diag}[I_{n_1}, I_{n_2}, -I_{n_3}, I_{n_4}, \ldots, -I_{n_{2i+1}}, I_{n_{2i+2}}, \ldots]$$

have positive trace and are thus similar to elements of $\Gamma^*(G)$; the same holds for their product. So $C = U\,\mathrm{diag}[I_{n_1}, I_{n_2}, -I_{n_3}, \ldots, -I_{n_k}]U^{-1}$ is in $\Gamma^*(G)$ which implies $BC = U\,\mathrm{diag}[-I_{n_1}, I_{n_2}, -I_{n_3}, \ldots, -I_{n_k}]U^{-1}$ is in $\Gamma^*(G)$. But this is impossible since tr BC is negative. Thus we have shown that in the case $|\Gamma(G)| = 2^{k-1}$ the elements of $\Gamma^*(G)$ are those and only those of the form

$$U\,\mathrm{diag}[I_{n_1}, B_2, \ldots, B_k]U^{-1}, \text{ where } B_i \text{ is } I_{n_i} \text{ or } -I_{n_i} \text{ for } 2 \le i \le k.$$

Now let $\gamma_i (2 \le i \le k)$ be the elements of $\Gamma(G)$ for which $P(\gamma_i) = U[\mathrm{diag}\, I_{n_1}, I_{n_2}, \ldots, -I_{n_i}, \ldots, I_{n_k}]U^{-1}$. Clearly, $\Gamma(G)$ is the direct product of $k-1$ cyclic subgroups of order 2 having the elements γ_i as generators. Since tr $P(\gamma_i) = n_1 + n_2 + \ldots - n_i + \ldots + n_k$, there are $2n_i$ points fixed by γ_i. Similarly, if we consider the product $\gamma_i\gamma_j$ $(i \ne j)$ of two generators, we see that there are $2(n_i + n_j)$ points fixed by $\gamma_i\gamma_j$. But this implies that for each point v of G, there is at most one i $(2 \le i \le k)$ such that $\gamma_i(v) \ne v$. Hence, for each $\gamma \in \Gamma(G)$ either $\gamma(v) = v$ or $\gamma(v) = \gamma_i(v)$ and the theorem follows.

Let G be a graph for which case A holds. Suppose the characteristic polynomial of G splits over the integers into k distinct, irreducible factors of degrees $n_1 \ge n_2 \ge \ldots \ge n_k$, respectively.

<u>Corollary 3.1.</u> Let n_1 be as above. Under the hypotheses of the theorem, n_1 equals the number of orbits of $\Gamma(G)$.

Proof. The number of orbits of $\Gamma(G)$ is given by Burnside's Lemma to be

$$\frac{1}{|\Gamma(G)|} \sum_{\gamma\varepsilon\Gamma(G)} tr(P(\gamma)) = \frac{1}{2^{k-1}} 2^{k-1} n_1 = n_1 \text{ , as required.}$$

If G is such that case A holds, the following observations also obtain. The set of points of G can be decomposed into k pointwise disjoint subsets V_i such that

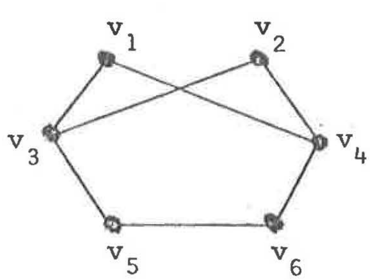
$$|V_1| = n_1 - n_2 - \ldots - n_k$$
$$|V_i| = 2n_i, \ i=2,\ldots,k$$

where V_1 consists of those points v of G satisfying $\gamma(v) = v$ for each $\gamma\varepsilon\Gamma(G)$, and V_i $(2\leq i\leq k)$ contains n_i pairs of points representing the orbits of the generator γ_i.

Corollary 3.2. Let G be an n-point graph with non-derogatory adjacency matrix, and let $n_1 \geq n_2 \geq \ldots \geq n_k$ be the degrees of the irreducible factors of its minimal polynomial. If $n_1 < \frac{n}{2}$, then G satisfies case B.

Proof. If $|\Gamma(G)| = 2^{k-1}$ then it follows from Theorem 3 and Corollary 3.1 that n_1, the number of orbits of $\Gamma(G)$, must be greater than or equal to $\frac{n}{2}$.

Some examples follow. For the graph G of Figure 1, $n_1=3$ and $n_2=n_3=1$; $\Gamma(G)$ has three orbits $\{v_1,v_4\}$, $\{v_2,v_3\}$, $\{v_5\}$ equal respectively to V_1, V_2, V_3. Figure 2 exhibits a 6-point graph satisfying case A. Here $n_1=3$, $n_2=2$, $n_3=1$ and $|\Gamma(G)|=4$.



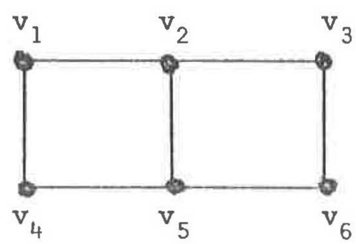
$$\phi_G(x) = (x^3-x^2-5x+4)(x^2+x-1)x$$

$$\Gamma(G) = \{e, (v_1v_2), (v_3v_4)(v_5v_6), (v_1v_2)(v_3v_4)(v_5v_6)\}$$

Figure 2

$\Gamma(G)$ has three orbits $\{v_1,v_2\}$, $\{v_3,v_4\}$, $\{v_5,v_6\}$; V_1 is empty because $n_3-n_2-n_1=0$, $V_2 = \{v_3,v_4,v_5,v_6\}$, the union of two orbits, and $V_3 = \{v_1,v_2\}$, the remaining orbit. For the graph H of Figure 1, $n_1 = 2 < \frac{5}{2}$ and $|\Gamma(G)| = 2 < 2^{k-1} = 4$.

Case B is more difficult to analyze. The results obtained in case A do not apply as can be seen from the graph H in Figure 1 or the graph in Figure 3.



$\phi_G(x) = (x^2+2x-1)(x^2-2x-1)(x-1)(x+1)$

$\Gamma(G) = \{e,(v_1v_3)(v_4v_6),(v_1v_4)(v_2v_5)(v_3v_6),$
$(v_1v_6)(v_3v_4)(v_2v_5)\}$

Figure 3

In this last example we have $\Gamma(G) = 4 = 2^{k-2}$ and the orbits are $\{v_1,v_3,v_4,v_6\}$ and $\{v_2,v_5\}$.

2. Point-Symmetric Graphs

Let G be a p-point graph with automorphism group $\Gamma(G)$; let Γ_{v_i} $(v_i \in V(G))$ denote the stabilizer of v_i, and $O(\Gamma_{v_i})$ the number of orbits of Γ_{v_i}.

A graph G is said to be point-symmetric if its automorphism group is transitive - obviously, $O(\Gamma_{v_i}) = O(\Gamma_{v_j})$ $(1 \le i,j \le p)$ in this case. By Theorem 1 $\deg \mu_G \le \sum_{i=1}^{r} e_i \le \sum_{i=1}^{r} e_i^2$. But $\sum_{i=1}^{r} e_i^2$ is the order of the algebra Δ of all matrices commuting with all elements of $\Gamma^* = \{P(\gamma) \mid \gamma \in \Gamma(G)\}$. According to a theorem of Schur [10], if Γ^* is transitive, the order of Δ is also equal to the number of orbits of the stabilizer of any given element. Therefore we obtain the following.

Corollary 3.3. If G is a point-symmetric graph, then $\deg \mu_G \le O(\Gamma_{v_i})$.

Now let G be a PPS-graph (ie a point-symmetric graph with a prime number of points). In this case the minimal polynomial of G completely determines $\Gamma(G)$, as will be shown in the sequel. First, we introduce the following definition due to Turner [12]:

Definition. A p-point graph G is a starred polygon if its points can be labelled in such a way that

1) $[v_0, v_1] \in E(G)$
2) $[v_i, v_j] \in E(G)$ iff $[v_{\rho(i+k)}, v_{\rho(j+k)}] \in E(G)$ for $1 \le k \le p-1$ where $\rho(q)$ denotes the remainder on division of q by p, ie
   $\rho(q) \equiv q \pmod{P}$ and $0 \le \rho(q) < p$.

Turner [12] showed that a non-trivial graph with a prime number of points is a PPS-graph iff it is a starred polygon. Now, as Turner points out, the adjacency matrix of a starred polygon is a circulant matrix. We can therefore write the adjacency matrix of a non-trivial PPS-graph in the following way.

$$A(G) = \begin{vmatrix} 0 & a_1 & a_2 & \cdots & a_{p-1} \\ a_{p-1} & 0 & a_1 & & a_{p-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & & 0 \end{vmatrix}$$

where $a_1 = 1$.

It is well-known that the eigenvalues of such a matrix are given by

$$\alpha_k = \sum_{j=1}^{p-1} a_j \omega^{\rho(jk)} \qquad (0 \le k \le \rho-1)$$ where ω is a primitive p^{th} root of unity.

$\alpha_0 = \sum_{j=1}^{p-1} a_j$ is exactly the degree of G, while all the other eigenvalues are non-integer values.

Theorem 3. Let m be the multiplicity of the eigenvalue α_1. Then the order of Γ_{v_0}, the stabilizer of the element v_0, is equal to m.

Proof. If $\alpha_k=\alpha_1$, then $\sum_{j=1}^{p-1} a_j\omega^{\rho(jk)} = \sum_{j=1}^{p-1} a_j\omega^j$; but since the primitive roots of unity are linearly independent over the rationals, this is possible iff $a_j = a_{\rho(jk)}$ $(1\le j\le p-1)$. However, this is equivalent to the condition: $[v_0,v_j] \in E(G)$ iff $[v_0,v_{\rho(jk)}] \in E(G)$; and this in turn holds iff the permutation τ defined by $\tau(v_i) = v_{\rho(ki)}$ (for $v_i \in V$) is in Γ_{v_0}.

Corollary 3.1. Let G be a non-trivial p-point PPS-graph. Then $\deg \mu_G = 1 + \frac{p-1}{m}$.

Proof. Let $\alpha_h\neq\alpha_1$. Then $\alpha_{\rho(hk)} = \Sigma a_j\omega^{\rho(j\rho(hk))}$. Now if $\alpha_k=\alpha_1$ then $a_j=a_{\rho(jk)}$, $1\le j\le p-1$; hence $\alpha_{\rho(hk)} = \sum_{j=1}^{p-1} a_{\rho(jk)}\omega^{\rho(h\rho(jk))} = \sum_{j=1}^{p-1} a_j\omega^{\rho(jh)} = \alpha_h$. Therefore if m eigenvalues are equal to α_1, m eigenvalues are equal to α_h, and the number of distinct, non-integer valued eigenvalues of A(G) is given by p-1 divided by m, from which the corollary follows.

Corollary 3.2. Let G be a non-trivial PPS-graph of order p. Then

$$|\Gamma(G)| = \frac{p(p-1)}{\deg \mu_G - 1}$$

Proof. From the definition of starred polygon, it is evident that

$$|\Gamma_{v_i}| = |\Gamma_{v_0}| \quad (1\le i\le p-1).$$ Hence

$$|\Gamma(G)| = p|\Gamma_{v_0}| = \frac{p(p-1)}{\deg \mu_G - 1} .$$

3. An Algorithm for Determining the Automorphism Group of a PPS-Graph.

Both Alspach [1] and Chao and Wells [4] have presented algorithms for determining the automorphism group of a PPS-graph. Here, using the basic properties of a starred polygon, we give a simpler construction. If G is a PPS-graph of order p, let $\tau_{a,b}$ denote the permutation defined on V(G) by $\tau_{a,b}(v_i) = v_{\rho(ia+b)}$. Chao and Wells [4] have shown that $\Gamma(G) = \Gamma_{v_0} \times K$ where $K = \{\tau_{1,b} \mid 0 \le b \le p-1\}$. From Theorem 3 it follows that $\tau_{k,0} \in \Gamma_{v_0}$ iff $\alpha_k = \alpha_1$. Hence $\Gamma(G) = \{\tau_{k,b} | \alpha_k = \alpha_1,\ 0 \le b \le p-1\}$, and consequently $\Gamma(G)$ is completely determined once we have found all integers k such that $\alpha_k = \alpha_1$.

The symbol S of a starred polygon is defined to be the set

$$S = \{i \le p-1 \mid [v_0, v_i] \in E(G)\}.$$

Applying Theorem 3, we see that $\alpha_k = \alpha_1$ iff $\{\rho(jk) \mid j \in S\} = S$. Since $1 \in S$ (by definition of starred polygon), $k \in S$; by the same token, $i \in S$ iff $(p-i) \in S$. Now let $S' = \{i \in S \mid i \le \frac{p-1}{2}\}$ and let $k' \in S - S'$. Then $(p-k') \in S'$ and since $\rho(jk') = \rho(j(p-k')) = \rho(jp) - \rho(jk') = p - \rho(jk')$, we have $\rho(jk') \in S$ iff $[p-\rho(jk')] \in S$. From these observations it follows that in order to find those k such that $\alpha_k = \alpha_1$, one simply has to determine which elements $k \in S'$ are such that $\{\rho(jk) \mid j \in S'\} \subseteq S$. If k is one such element, then obviously both α_k and α_{p-k} are equal to α_1.

Example 1. (Alspach [1]) Let G be a graph with p=29, S = {1,3,5,12,17,24,26,28}. Since none of $\rho(3\times 3)$, $\rho(5\times 3)$, $\rho(12\times 3)$ is in S, m=2, and $|\Gamma(G)| = 58$. The elements of $\Gamma(G)$ are $\tau_{1,b}$, $\tau_{28,b}$ for $0 \le b \le p-1$.

Example 2. (Chao and Wells [4]) Let G be a graph with $p = 13$ and $S = \{1,5,8,12\}$. Since $\rho(5\times5) \in S$, $m = 4$ and $|\Gamma(G)| = 52$. The elements of $\Gamma(G)$ are $\tau_{1,b}$, $\tau_{5,b}$, $\tau_{8,b}$, $\tau_{12,b}$ for $0 \le b \le p-1$.

Example 3. Let G be a graph with $p=31$ and symbol $S=\{1,4,5,6,7,11,20,24,25,26,27,30\}$. $\rho(4\times4) \notin S$, but $\rho(5\times4)$, $\rho(5\times5)$, $\rho(5\times6)$, $\rho(5\times7)$, $\rho(5\times11)$ are all in S, as are also $\rho(6\times4)$, $\rho(6\times6)$, $\rho(6\times7)$, $\rho(6\times11)$. 7 and 11 can be disregarded because $\rho(7\times4) \notin S$ and $\rho(11\times4) \notin S$. Hence $m = 6$ and $|\Gamma(G)| = 186$. The elements of $\Gamma(G)$ are of the form $\tau_{1,b}$, $\tau_{5,b}$, $\tau_{6,b}$, $\tau_{30,b}$, $\tau_{26,b}$, $\tau_{25,b}$ for $0 \le b \le p-1$.

References

[1] Alspach, B. Point symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, J. of Combinatorial Theory (B) 15 (1973), 12-17.

[2] Boerner, H. Representation of Groups. Amsterdam: North-Holland, 1963.

[3] Chao, C.-Y. A note on the eigenvalues of a graph, J. of Combinatorial Theory (B) 3 (1971), 301-302.

[4] Chao, C.-Y. and Wells, J. G. A class of vertex-transitive digraphs, J. of Combinatorial Theory (B) 14 (1973), 246-255.

[5] Harary, F. Graph Theory. Reading, Mass.: Addison-Wesley, 1969.

[6] Curtis, W. C. and Reiner, I. Representation Theory of Finite Groups and Associative Algebras. Pure and Applied Mathematics, Vol. XI. New York: Wiley, 1962.

[7] Mowshowitz, A. The group of a graph whose adjacency matrix has all distinct eigenvalues, in: Proof Techniques in Graph Theory (F Harary, ed.). New York: Academic Press, 1969.

[8] Mowshowitz, A. The adjacency matrix and the group of a graph, in: New Directions in the Theory of Graphs (F. Harary, ed.). New York: Academic Press, 1973.

[9] Petersdorf, M. and Sachs, H. Spektrum und Automorphismengruppen eines Graph, in: Combinatorial Theory and its Applications (edited by P. Erdos, et al.). Amsterdam: North-Holland, 1969.

[10] Schur, I. Zur Theorie der einfach transitiven Permutationsgruppen, S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598-623.

[11] Suprunenko, D. A. and Tyshkevich, R. I. Commutative Matrices. New York: Academic Press, 1968.

[12] Turner, J. Point symmetric graphs with a prime number of points, J. of Combinatorial Theory. 3 (1967), 136-145.

[13] Wielandt, H. Finite Permutation Groups. New York: Academic Press, 1964.