View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

JOURNAL OF COMBINATORIAL THEORY, Series B 26, 309–316 (1979)

On Regular Graphs, VI*

DRAGOMIR Ž. DJOKOVIĆ

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1 Canada

Communicated by the Editors

Received August 10, 1976

Let G be a connected regular graph of valence $p + 1$ where p is an odd prime. Let A be a subgroup of Aut(G) which is s-regular ($s \geqslant 0$). We prove that $s \leqslant 3$ and the cases $s = 0, 1, 2, 3$ do occur.

1. MAIN RESULT

In the whole paper G denotes a connected regular graph (finite or infinite) of valence $p + 1$ where p is an odd prime. We assume that there is a subgroup A of Aut (G) which is s-regular for some $s \geqslant 0$.

We have proved in [3] that $s \leqslant 7$ and $s \neq 6$. A short beautiful proof of a more general result (the valence being replaced by $p^k n + 1$ where $n < p$, $k \geqslant 1$) was given later by R. M. Weiss [5]. We also proved [4] that if $s \geqslant 2$ then the prime p must be a Mersenne prime, i.e., $p + 1 = 2^n$ for some positive integer n.

In this paper we finish off this problem by proving the following:

THEOREM. *Under the above hypotheses we have* $s \leqslant 3$.

2. PROOF OF $s \neq 7$

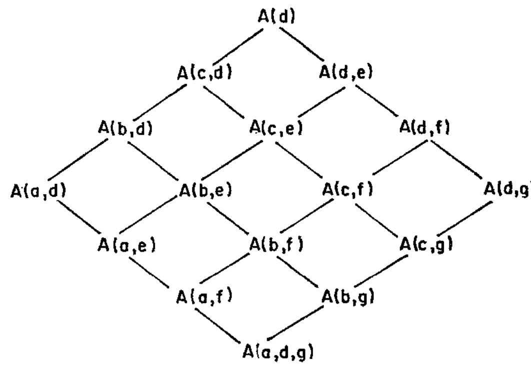
Assume that $s = 7$. Let a, b, c, d, e, f, g be consecutive vertices of a 6-arc S in G. If $v_1, \ldots, v_k$ are vertices of G we denote by $A(v_1, \ldots, v_k)$ the subgroup of A consisting of all $\alpha \in A$ such that $\alpha(v_i) = v_i$, $1 \leqslant i \leqslant k$ and we say that this subgroup is *the fixer* in A of the set $\{v_1, \ldots, v_k\}$. On the other hand, the *stabilizer* of $\{v_1, \ldots, v_k\}$ in A is the subgroup of A consisting of all $\alpha \in A$ such that $\{\alpha(v_1), \ldots, \alpha(v_k)\} = \{v_1, \ldots, v_k\}$. It is clear that a fixer in A of a set of vertices is a normal subgroup of the stabilizer in A of the same set of vertices.

* This work was supported in part by NRC Grant A-5285.

0095-8956/79/030309–08$02.00/0

Copyright © 1979 by Academic Press, Inc.
All rights of reproduction in any form reserved.

We have the following diagram of various fixers:



Note that the girth of G is $\geqslant 2s - 2 = 12$ and consequently $A(b, d) = A(b, c, d)$, $A(a, d) = A(a, b, c, d)$, etc. (See [1] Prop. 17.2, p. 113).

Since A is 7-regular the orders of all subgroups in this diagram are known:

$$|A(d) = (p + 1)\,p^6,$$
$$|A(c, d)| = p^6, \; |A(c, e)| = p^5,$$
$$|A(b, e)| = p^4, \; |A(b, f)| = p^3,$$
$$|A(a, f)| = p^2, \; |A(a, d, g)| = p$$

The subgroups in the same row of this diagram (say $A(c, d)$ and $A(d, e)$) are conjugate in A to each other.

It follows from [3, section 4] that the groups $A(a, d)$, $A(b, e)$, $A(c, f)$, $A(d, g)$ are elementary abelian but the groups $A(b, d)$, $A(c, e)$, $A(d, f)$ are non-abelian. In fact when $s = 7$ the inequality

$$\tfrac{2}{3}(s - 1) \leqslant k < \tfrac{1}{2}(s + 2)$$

from [3, p. 259] gives $k = 4$. This means that the fixer in A of a 3-arc $(3 = s - k)$ is abelian (necessarily elementary abelian) but the fixer in A of a 2-arc is not abelian.

Since $A(c, e)$ is generated by $A(b, e)$ and $A(c, f)$ the above facts imply that $A(b, f)$ is the center of $A(c, e)$. This follows also from Lemma 2 of [3]. Moreover, that Lemma gives that the center of $A(c, d)$ is $A(a, f)$ and the center of $A(d)$ is $A(a, d, g)$.

For each vertex v of G let $Z(v)$ be the center of $A(v)$. We have just seen that $Z(v)$ coincides with the fixer in A of any 6-arc S such that $S(3) = v$. Hence we have

LEMMA 1. *$Z(v)$ consists of all $\alpha \in A(v)$ which fix every vertex at distance $\leqslant 3$ from v. If $\alpha \in Z(v)$, $\alpha \neq 1$ then α moves every vertex at distance 4 from v.*

Proof. The first statement had been proved above. The second follows from 7-regularity of A.

Given a vertex v of G we shall denote by $\tilde{v}$ a fixed nontrivial element of $Z(v)$.

LEMMA 2. *We have*

$$\begin{aligned} A(a, d, g) &= Z(d) = \langle \tilde{d} \rangle, \\ A(a, f) &= \langle \tilde{c}, \tilde{d} \rangle, \\ A(b, f) &= \langle \tilde{c}, \tilde{d}, \tilde{e} \rangle, \\ A(b, e) &= \langle \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e} \rangle, \\ A(c, e) &= \langle \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e}, \tilde{f} \rangle, \\ A(c, d) &= \langle \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e}, \tilde{f} \rangle, \\ A(d) &= \langle \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e}, \tilde{f}, \tilde{g} \rangle. \end{aligned}$$

Proof. Since $Z(d)$, has order p and $\tilde{d} \neq 1$ is in $Z(d)$ we have $Z(d) = \langle \tilde{d} \rangle$.

Clearly, $\tilde{c}, \tilde{d} \in A(a, f)$ by Lemma 1 and hence $\langle \tilde{c}, \tilde{d} \rangle \subset A(a, f)$. Since both $\langle \tilde{c}, \tilde{d} \rangle$ and $A(a, f)$ have order p^2 they are equal. All other equalities can be proved similarly.

We denote by $(x, y) = xyx^{-1}y^{-1}$ the commutator of two elements x, y of a group.

LEMMA 3. *We have* $(\tilde{b}, \tilde{f}) = \tilde{d}^r$ *for some* $r \not\equiv 0 \pmod p$.

Proof. $(\tilde{b}, \tilde{f}) \neq 1$ because $A(c, e)$ is non-abelian. An easy inspection shows that $(\tilde{b}, \tilde{f})$ fixes a and g and hence belongs to the fixer of S, i.e., to $Z(d)$.

LEMMA 4. *We have*

$$(\tilde{a}, \tilde{f}) \in \langle \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e} \rangle = A(b, e)$$

but

$$(\tilde{a}, \tilde{f}) \notin \langle \tilde{c}, \tilde{d}, \tilde{e} \rangle = A(b, f).$$

Proof. By Lemma 1 the distance between $\tilde{f}^{-1}(b)$ and a is 3. Therefore $\tilde{a}^{-1}\tilde{f}^{-1}(b) = \tilde{f}^{-1}(b)$, $\tilde{f}\tilde{a}^{-1}\tilde{f}^{-1}(b) = b$ and $(\tilde{a}, \tilde{f})(b) = \tilde{a}(b) = b$. Thus $(\tilde{a}, \tilde{f})$ fixes b and similarly, it fixes e.

On the other hand the distance between $\tilde{a}^{-1}(f)$ and f is 4. By Lemma 1 we have $\tilde{f}\tilde{a}^{-1}(f) \neq \tilde{a}^{-1}(f)$ and consequently

$$(\tilde{a}, \tilde{f})(f) = \tilde{a}\tilde{f}\tilde{a}^{-1}(f) \neq f.$$

Therefore $(\tilde{a}, \tilde{f}) \notin A(f)$ and $(\tilde{a}, \tilde{f}) \notin A(b, f)$.

Now, $A(c, e) \lhd A(d)$, see [4, section 5]. Since $A(b, f)$ is the center of $A(c, e)$ we have $A(b, f) \lhd A(d)$. Thus we have an action of $A(d)$ on $V = A(c, e)/A(b, f)$ induced by conjugation. For $\tau \in A(c, e)$ let $\hat{\tau}$ be its canonical image in V. Similarly, the canonical images of $\tilde{b}$ and $\tilde{f}$ in V will be denoted by $\hat{b}$ and $\hat{f}$, respectively. The above action of $A(d)$ on V is given explicitly as follows

$$\sigma * \hat{\tau} = (\sigma\tau\sigma^{-1})^{\wedge}$$

where $\sigma \in A(d)$ and $\tau \in A(c, e)$. Thus we use the star to denote this action. Note that the elements $\sigma \in A(c, e)$ act trivially on V, i.e., $\sigma * \hat{\tau} = \hat{\tau}$ for such σ and all $\tau \in A(c, e)$.

The fixer of $\{a, d, g\}$ is $Z(d) = \langle \tilde{d} \rangle$. The stabilizer of $\{a, d, g\}$ has order $2p$ because there exist automorphisms in A which map S to its opposite 6-arc. Let α be any element of order 2 in this stabilizer. Then we have

$$\alpha(a) = g, \ \alpha(b) = f, \ \alpha(c) = e.$$

From now on we shall assume that $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{e}, \tilde{f}, \tilde{g}$ have been chosen so that $\alpha\tilde{a}\alpha = \tilde{g}$, $\alpha\tilde{b}\alpha = \tilde{f}$, $\alpha\tilde{c}\alpha = \tilde{e}$. This can be done because we can use these equations to define $\tilde{g}, \tilde{f}, \tilde{e}$ in terms of $\tilde{a}, \tilde{b}, \tilde{c}$ which are still arbitrary.

Thus $\alpha * \hat{b} = \hat{f}$ and $\alpha * \hat{f} = \hat{b}$.

Let B be a Sylow 2-subgroup of $A(d)$ containing α. We know by [4, Theorem 4] that B is elementary abelian of order $2^n = p + 1$ and that $A(c, b)B \lhd A(d)$.

By Lemma 4 we have

$$\tilde{a}\tilde{f}\tilde{a}^{-1} \equiv \tilde{b}^k\tilde{f} \bmod A(b, f)$$

where $k \not\equiv 0 \pmod p$. Thus

$$\tilde{a} * \hat{f} = (\tilde{a}\tilde{f}\tilde{a}^{-1})^{\wedge} = \hat{b}^k\hat{f},$$
$$\tilde{a} * \hat{b} = (\tilde{a}\tilde{b}\tilde{a}^{-1})^{\wedge} = \hat{b}.$$

Since

$$\tilde{a}^{-1} = \tilde{a}^{p-1}$$

we have

$$\tilde{a}^{-1} * \hat{f} = (\hat{b}^k)^{p-1}\hat{f} = \hat{b}^{-k}\hat{f}.$$

Let $\beta = \tilde{a}\alpha\tilde{a}^{-1}$. Then

$$\begin{aligned} \alpha\beta * \hat{f} &= \alpha\tilde{a}\alpha\tilde{a}^{-1} * \hat{f} = \alpha\tilde{a}\alpha * (\hat{b}^{-k}\hat{f}) \\ &= \alpha\tilde{a} * (\hat{b}\hat{f}^{-k}) \\ &= \alpha * (\hat{b}(\hat{b}^k\hat{f})^{-k}) = \alpha * (\hat{b}^{1-k^2}\hat{f}^{-k}) \\ &= \hat{b}^{-k}(\hat{f})^{1-k^2} \end{aligned} \tag{1}$$

and

$$\begin{aligned}\beta\alpha * \hat{f} &= \beta * \hat{b} = \tilde{a}\alpha\tilde{a}^{-1} * \hat{b} = \tilde{a}\alpha * \hat{b} \\ &= \tilde{a} * \hat{f} = \hat{b}^k \hat{f}.\end{aligned} \tag{2}$$

But $\beta \in A(c, e)B$ because $\alpha \in B$ and $A(c, e)B \lhd A(d)$. We can write $\beta = \gamma\sigma$ with $\gamma \in A(c, e)$ and $\sigma \in B$. Since B is abelian, α and σ commute and hence

$$\begin{aligned}\alpha\beta * \hat{f} &= \alpha\gamma * (\sigma * \hat{f}) = \alpha * (\sigma * \hat{f}) \\ &= \alpha\sigma * \hat{f} = \sigma\alpha * \hat{f} = \gamma * (\sigma\alpha * \hat{f}) \\ &= \gamma\sigma\alpha * \hat{f} = \beta\alpha * \hat{f}\end{aligned} \tag{3}$$

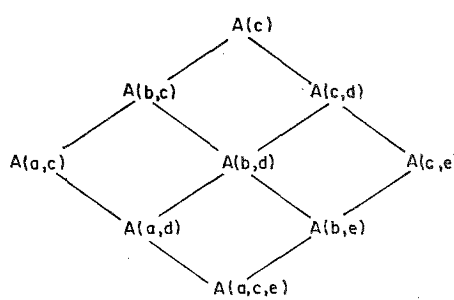
because $\gamma \in A(c, e)$ acts trivially on v.

From (1), (2) and (3) we obtain that $\hat{b}^{2k} = 1$, i.e., that p divides $2k$. This is a contradiction because p is an odd prime and we know that $k \not\equiv 0 \pmod{p}$.

Thus $s = 7$ is impossible.

3. Proof of $s \neq 5$

Assume that $s = 5$. Let a, b, c, d, e be consecutive vertices of a 4-arc S in G. Now we have the diagram



where $|A(c)| = (p+1)p^4$, $|A(b, c)| = p^4$, $|A(b, d)| = p^3$, $|A(a, d)| = p^2$, $|A(a, c, e)| = p$.

As in the previous case, one knows that $A(b, d)$ is elementary abelian, $A(b, c)$ is non-abelian, $A(a, d)$ is the center of $A(b, c)$ and $A(a, c, e)$ is the center of $A(c)$. Again we shall write $Z(c) = A(a, c, e)$. For each vertex v of G let $\tilde{v}$ be a non-trivial element of $Z(v)$, thus $Z(v) = \langle \tilde{v} \rangle$. The elements of $Z(v)$ fix every vertex of G at distance $\leqslant 2$ from v and this property characterizes $Z(v)$. Moreover, $\tilde{v}$ moves every vertex at distance 3 from v.

Again we have an element $\alpha \in A(c)$ such that $\alpha^2 = 1$, $\alpha(a) = e$ and $\alpha(b) = d$. We shall assume that $\tilde{a}$, $\tilde{b}$, $\tilde{d}$, $\tilde{e}$ have been chosen so that $\alpha\tilde{a}\alpha = \tilde{e}$ and $\alpha\tilde{b}\alpha = \tilde{d}$.

Note that we have

$$\begin{aligned} A(a, c, e) &= \langle \tilde{c} \rangle, \\ A(a, d) &= \langle \tilde{b}, \tilde{c} \rangle, \\ A(b, d) &= \langle \tilde{b}, \tilde{c}, \tilde{d} \rangle, \\ A(b, c) &= \langle \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \rangle, \\ A(c) &= \langle \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e} \rangle. \end{aligned}$$

Since $(\tilde{a}, \tilde{d}) \in A(a, d) = \langle \tilde{b}, \tilde{c} \rangle$ and since $(\tilde{a}, \tilde{d})$ moves e it follows that

$$\tilde{a}\tilde{d}\tilde{a}^{-1}\tilde{d}^{-1} \equiv \tilde{b}^k \qquad \text{mod } \langle \tilde{c} \rangle.$$

Now let $V = A(b, d)/A(a, c, e)$ and let $A(c)$ act on V by conjugation. Using the notation analogous to that which we used in the previous section, we have

$$\begin{aligned} \tilde{a} * \hat{b} = \hat{b}, \ \tilde{a} * \hat{d} = \hat{b}^k\hat{d}, \\ \alpha * \hat{b} = \hat{d}, \ \alpha * \hat{d} = \hat{b}. \end{aligned}$$

The elements of $A(b, d)$ act trivially in V.

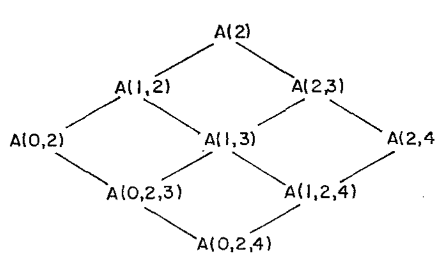
Let $\beta = \tilde{a}\alpha\tilde{a}^{-1}$. Then

$$\begin{aligned} \alpha\beta * \hat{d} &= \alpha\tilde{a}\alpha\tilde{a}^{-1} * \hat{d} = \alpha\tilde{a}\alpha * (\hat{b}^{-k}\hat{d}) \\ &= \alpha\tilde{a} * (\hat{b}\hat{d}^{-k}) = \alpha * (\hat{b}(\hat{b}^k\hat{d})^{-k}) \\ &= \alpha * ((\hat{b})^{1-k^2}\, \hat{d}^{-k}) \\ &= \hat{b}^{-k}(\hat{d})^{1-k^2}, \\ \beta\alpha * \hat{d} &= \beta * \hat{b} = \tilde{a}\alpha\tilde{a}^{-1} * \hat{b} = \tilde{a}\alpha * \hat{b} \\ &= \tilde{a} * \hat{d} = \hat{b}^k\hat{d}. \end{aligned}$$

We get now a contradiction in the same way as in section 2.

4. Proof of $s \neq 4$

Assume that $s = 4$. Let 0, 1, 2, 3, 4 be consecutive vertices of a 4-arc in G. Denote the edges {0, 1}, {1, 2}, {2, 3}, {3, 4} by a, b, c, d, respectively. The girth of G is $\geqslant 6$. We now have the diagram



where $A(0, 2, 4)$ is the trivial group. The orders are given by

$$|A(2)| = (p+1)p^3,\ |A(1, 2)| = p^3,$$
$$|A(1, 3)| = p^2,\ |A(0, 2, 3)| = p.$$

It follows from [3, Lemma 2] that $A(0, 2, 3)$ is the center of $A(1, 2)$ and $A(0, 2, 4)$ is the center of $A(2)$.

LEMMA 5. *The elements of* $A(0, 2, 3)$ *are characterized by the property that they fix every vertex at distance* ≤ 1 *from the edge* b. *Moreover, if* $\tilde{b}$ *is any non-trivial element of* $A(0, 2, 3)$ *then* $\tilde{b}$ *moves every vertex at distance* 2 *from the edge* b.

Proof. Let $\alpha \in A(0, 2, 3)$ and let 5 be a vertex at distance 1 from b, say 5 is adjacent to 1. By 4-regularity of A there exists $\beta \in A(1, 2)$ such that $\beta(0) = 5$. Then since α belongs to the center of $A(1, 2)$ we have $\alpha\beta = \beta\alpha$ and $\alpha(5) = \alpha\beta(0) = \beta\alpha(0) = \beta(0) = 5$. This proves the first assertion. The second follows from the 4-regularity of A.

Now, it is easy to check that

$$\begin{aligned} A(0, 2, 3) &= \langle \tilde{b} \rangle, \\ A(1, 3) &= \langle \tilde{b}, \tilde{c} \rangle, \\ A(1, 2) &= \langle \tilde{a}, \tilde{b}, \tilde{c} \rangle, \\ A(2) &= \langle \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \rangle. \end{aligned}$$

From now on let $\alpha \in A(2)$ be defined by $\alpha(0) = 4$, $\alpha(4) = 0$. Then $\alpha^2 = 1$, $\alpha \neq 1$. We assume that $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$ have been chosen so that $\alpha\tilde{a}\alpha = \tilde{d}$, $\alpha\tilde{b}\alpha = \tilde{c}$.

The group $A(2)$ acts on $A(1, 3)$ by conjugation

$$\sigma * \tau = \sigma\tau\sigma^{-1}$$

for $\sigma \in A(2)$ and $\tau \in A(1, 3)$.

The commutator $(\tilde{a}, \tilde{c})$ is not the identity because $A(1, 2)$ is non-abelian. Hence $(\tilde{a}, \tilde{c}) = \tilde{b}^k$ for some $k \not\equiv 0 \pmod p$.

Thus we have

$$\tilde{a} * \tilde{b} = \tilde{b},\ \tilde{a} * \tilde{c} = \tilde{b}^k\tilde{c},$$
$$\alpha * \tilde{b} = \tilde{c},\ \alpha * \tilde{c} = \tilde{b}.$$

Let $\beta = \tilde{a}\alpha\tilde{a}^{-1}$. Then

$$\begin{aligned} \alpha\beta * \tilde{c} &= \alpha\tilde{a}\alpha\tilde{a}^{-1} * \tilde{c} = \alpha\tilde{a}\alpha * (\tilde{b}^{-k}\tilde{c}) \\ &= \alpha\tilde{a} * (\tilde{b}\tilde{c}^{-k}) = \alpha * (\tilde{b}(\tilde{b}^k\tilde{c})^{-k}) \\ &= \alpha * ((\tilde{b})^{1-k^2}\tilde{c}^{-k}) = \tilde{b}^{-k}(\tilde{c})^{1-k^2}, \\ \beta\alpha * \tilde{c} &= \beta * \tilde{b} = \tilde{a}\alpha\tilde{a}^{-1} * \tilde{b} = \tilde{a}\alpha * \tilde{b} \\ &= \tilde{a} * \tilde{c} = \tilde{b}^k\tilde{c}. \end{aligned}$$

Now, we get a contradiction in the same way as in section 2. This completes the proof of our Theorem.

5. Some Examples

Now we shall show that the cases $s = 1, 2, 3$ can occur by constructing few simple examples. The case $s = 0$ is well-known to occur since we can use Cayley graphs as examples.

Example 1. Let P be a sharply doubly transitive subgroup of the symmetric group S_n. It is well-known [2, section 20.7] that n must be a power of a prime, say, $n = q^k$, q prime, $k \geqslant 1$. Let $V = \{1, 2, ..., n\}$ be the set on which P acts. Let P' be another copy of P and $V' = \{1', 2', ..., n'\}$ another copy of V and we assume that P' acts on V'. Let $G = K_{n,n}$ be the complete bipartite graph whose vertex set is the disjoint union $V \cup V'$; two vertices being adjacent only if one of them is in V and the other in V'. Let A be the subgroup of $Aut(G)$ which is generated by P, P' and the involution $y = (11')(22') \cdots (nn')$. It is clear that A is 3-regular.

The valence of G is $n = q^k$. This will be of the form $p + 1$, p prime, if and only if $q = 2$ and $p = 2^k - 1$ is a Mersenne prime.

Example 2. Let P be a sharply transitive subgroup of S_n. Define G and A as in Example 1. Then A is 1-regular.

Example 3. Let $G = K_5$. Then $\mathrm{Aut}(G) = S_5$ has a subgroup $A = A_5$ of index 2. This A is 2-regular

References

1. N. Biggs, "Algebraic Graph Theory," Cambridge Univ. Press, London/New York, 1974.
2. M. Hall, Jr., "The Theory of Groups," Macmillan Co., New York, 1959.
3. D. Ž. Djoković, On regular graphs II, *J. Combinatorial Theory Ser. B* **12** (1972), 252–259.
4. D. Ž. Djoković, On regular graphs IV, *J. Combinatorial Theory Ser. B* **15** (1973), 167–173.
5. R. M. Weiss, Über s-reguläre Graphen, *J. Combinatorial Theory Ser. B* **16** (1974), 229–233.