COMPOSITIO MATHEMATICA

LÁSZLÓ BABAI

On a conjecture of M. E. Watkins on graphical regular representations of finite groups

Compositio Mathematica, tome 37, nº 3 (1978), p. 291-296

<http://www.numdam.org/item?id=CM_1978__37_3_291_0>

COMPOSITIO MATHEMATICA, Vol. 37, Fasc. 3, 1978, pag. 291–296
Sijthoff & Noordhoff International Publishers – Alphen aan den Rijn
Printed in the Netherlands

ON A CONJECTURE OF M.E. WATKINS ON GRAPHICAL REGULAR REPRESENTATIONS OF FINITE GROUPS

László Babai

1. Introduction

For G a group, let $G_L = \{\lambda_g : g \in G\}$ denote the group of left translations of G. Thus λ_g is a permutation of the set G acting as $\lambda_g x = gx$ $(x \in G)$ for each $g \in G$. The graph X is a *graphical regular representation* (GRR) of G if the vertex set of X is $V(X) = G$, and the automorphism group of X, Aut X coincides with G_L. The problem of determining which groups admit a GRR has been the object of a great number of papers in the recent years (cf. [7] for a survey and [1, 2, 4] for more recent development).

M.E. Watkins [5] defined the following classes of groups: *Class I* consists of those finite groups which admit a GRR.

A finite group G belongs to *Class II*, if for each subset $H \subseteq G$, satisfying $H = H^{-1}$, there exists a non-identity automorphism ϕ of G such that $\phi H = H$. (This was originally required for generating sets H only; but $\phi H = H$ implies $\phi(G \setminus H) = G \setminus H$ hence this formulation yields the same class.)

A non-abelian group G is a *generalized dicyclic group*, if G has an abelian normal subgroup A of index 2 such that for some (actually any) $b \in G \setminus A$,

$$b^4 = e \text{ (the unit element of } G); \quad b^2 \neq e;$$

$$a^b = a^{-1} \text{ for any } a \in A.$$

(a^b denotes $b^{-1}ab$).

Let us define *Class III* as the class of all finite abelian and generalized dicyclic groups, except the elementary abelian 2-groups.

THEOREM 1: (*Tekla Lewin and M.E. Watkins* [5]). *A finite group G belongs to Class III if and only if there exists a non-identity automorphism ϕ of G such that $\phi x \in \{x, x^{-1}\}$ for any $x \in G$.*

This in turn implies that Class III is a subclass of Class II. It is easily seen that Class I and Class II are disjoint ([5]). Watkins proposed the following two conjectures:

CONJECTURE A (1970) [5, p. 97]: *The union of Class I and Class II includes all finite groups.*

CONJECTURE B (1973) [6, p. 50]: *There exists a positive integer N such that if a non-abelian group G is in Class II, then G is a generalized dicyclic group, or $|G| \leq N$.*

Let Z_m denote the cyclic group of order m; and $G^m = G \times \cdots \times G$ (m times).

As the abelian members of Class II are Z_2^2, Z_2^3, Z_2^4 and the abelian members of Class III ([3]), this conjecture can equivalently be formulated as

CONJECTURE B′: *There exists an integer N such that no group of order exceeding N belongs to the difference Class II\Class III.*

Later Watkins recalled this conjecture in the following formulation:

CONJECTURE C (1975) [7, p. 518]: *There exists an integer N such that if $|G| > N$ then G is abelian or G is generalized dicyclic or G admits a GRR.*

This is clearly a strong conjecture; its solution would (at least in principle) settle the GRR-problem. It is far from being equivalent to B. In fact, it is clearly equivalent to the conjunction of B and the following, somewhat weaker form of A:

CONJECTURE A′: *The union of Class I and Class II contains all finite groups of order exceeding some integer N.*

From [7] we learn that Watkins "has been plagued intermittently with doubts ever since" he has formulated B. Apparently, he found A′ to be more plausible. The aim of the present note is to prove B.

THEOREM 2: *If a non-abelian finite group G with $|G| \geq 4683$ belongs to Class II then G is generalized dicyclic.*

Equivalently, we assert that B and B′ hold with $N = 4682$. This implies that A′ and C are equivalent (and, consequently, A implies C).

Let us close this section with conjecturing that the same holds if G is an arbitrary non-abelian infinite group.

2. The proof

By the *orbits* of a permutation ψ we mean the orbits of the cyclic group $\langle\psi\rangle$ generated by ψ. Fixed letters are one-element orbits. The following are straightforward:

PROPOSITION: (a) *If a permutation ψ, acting on some set K, has ℓ orbits, then the number of subsets of K, invariant under ψ, is 2^ℓ.*

(b) *Setting $|K| = k$, the number of letters fixed by ψ is at least $2\ell - k$.* ■

We shall need the following lemma:

LEMMA 1: *Let P be a set of permutations, acting on a set K. Let $|K| = k$ and $\log_2 |P| = p$. Assume that for any subset L of K there is a member ϕ_L of P such that $\phi_L L = L$. Then there is a member ψ of P which fixes at least $k - 2[p]$ letters.*

PROOF: The proof is shorter than the lemma. K has 2^k subsets, hence there is a $\psi \in P$ such that at least $2^k/|P| = 2^{k-p}$ subsets are invariant under ψ. Let ℓ denote the number of orbits of ψ. Then, clearly, ψ has exactly 2^ℓ invariant subsets, whence $\ell \geq k - [p]$. This in turn implies that ψ fixes at least $2\ell - k \geq k - 2[p]$ letters (Prop. (b)). ■

COROLLARY: *Let G be a group of order n. Set $|\mathrm{Aut}\, G| = m + 1$, $\log_2 m = q$. If G belongs to Class II, then G has a non-identity automorphism ϕ and a subset D such that $|D| \leq 4[q]$ and $\phi x \in \{x, x^{-1}\}$ for each $x \in G \setminus D$.*

PROOF: Let L denote the set of pairs $\{x, x^{-1}\} (x \in G, x \neq e)$, and let P be the set of those permutations of L induced by the non-identity automorphisms of G. Clearly, $|P| \leq m$. Hence, an application of

Lemma 1 yields a $\psi \in P$ fixing at least $|L| - 2[q]$ letters. Let ψ be induced by $\phi \in \mathrm{Aut}\, G$ ($\phi \neq id$). By the definition of L this means that $\phi x \in \{x, x^{-1}\}$ for all but at most $4[q]$ members x of G. ■

LEMMA 2: *Let G be a group of order n and $D \subseteq G$ a subset of size $|D| < n/4$. Assume that for some $\phi \in \mathrm{Aut}\, G$, $\phi x = x^{-1}$ for each $x \in G \setminus D$. Then G is abelian.*

PROOF: Let $x \in G \setminus D$. We prove that x belongs to $Z(G)$, the center of G. This in turn implies that $G = Z(G)$ whence the lemma.

Assume to the contrary that $|C(x)| \leq n/2$ where $C(x)$ denotes the centralizer of x. Let $y \in G \setminus (C(x) \cup D \cup x^{-1}D)$. (The right-hand side is non-empty, since $|D| < n/4$.) Now $x, y, xy \in G \setminus D$, hence $\phi x = x^{-1}$, $\phi y = y^{-1}$ and $\phi(xy) = (xy)^{-1}$. On the other hand, $\phi(xy) = (\phi x)(\phi y) = x^{-1}y^{-1}$, whence $(xy)^{-1} = x^{-1}y^{-1}$, thus $y \in C(x)$, a contradiction with the choice of y. ■

LEMMA 3: *Let G be a group of order n and $D \subseteq G$ a subset of size $|D| < n/8$. Assume that there exists a non-identity automorphism ϕ of G such that $\phi x \in \{x, x^{-1}\}$ for each $x \in G \setminus D$. Then G belongs to Class III.*

PROOF: We break up the proof to a series of minor assertions. Let $A = \{x : x \in G, \phi x = x\}$, and $B = G \setminus (A \cup D)$. We may assume that A and D are disjoint.

I. *A is a proper subgroup of G, hence $|B| > 3n/8 > 3|D|$.*

II. *If $a \in A$, $b \in B \setminus a^{-1}D$ then $a^b = a^{-1}$.* (a^b stands for $b^{-1}ab$.)

PROOF: $ab \in aB \setminus D$, hence $ab \notin A \cup D$. Thus $ab \in B$, and (by the definition of B) $\phi(ab) = (ab)^{-1}$. On the other hand, $\phi(ab) = (\phi a)(\phi b) = ab^{-1}$. Comparing the results, $a^b = a^{-1}$ follows.

III. *A is abelian.*

PROOF: Let $a_1, a_2 \in A$ and $b \in B \setminus (a_1^{-1}D \cup a_2^{-1}D \cup (a_1a_2)^{-1}D)$. (The right-hand side is non-empty by I.) Hence, by II, $a_i^b = a_i^{-1}$ ($i = 1, 2$), $(a_1a_2)^b = (a_1a_2)^{-1}$. On the other hand, $(a_1a_2)^b = a_1^b a_2^b = a_1^{-1}a_2^{-1}$, hence a_1 and a_2 commute.

IV. *For any $a \in A$ and $x \in G$ we have $a^x \in \{a, a^{-1}\}$ and hence $|G : C(a)| \leq 2$. Moreover, $a^2 = e$ if and only if $a \in Z(G)$.* ($C(a)$ denotes the centralizer of a in G and $Z(G)$ the center of G.)

PROOF: Let N_a denote the normalizer of the set $\{a, a^{-1}\}$ in G. By III, $A \leq N_a$, and by II, $B \setminus a^{-1}D \subseteq N_a$. We conclude that $|N_a| \geq |A \cup (B \setminus a^{-1}D)| \geq n - 2|D| > n/2$, hence $N_a = G$. If $a^2 = e$ then $C(a) = N_a$ proving that $a \in Z(G)$. If $a^2 \neq e$ then $N_a \neq C(a)$ by II, hence $|N_a : C(a)| = 2$.

V. *If* $|G : A| = 2$ *then* G *belongs to Class III.*

PROOF: We assert that $\phi x \in \{x, x^{-1}\}$ for each $x \in G$. This, by Theorem 1, implies our statement. For $x \in A \cup B$, $\phi x \in \{x, x^{-1}\}$ by definition. Let $x \in D$, $b \in B$ and $a = b^{-1}x$. Clearly, $a \in A$. By IV, $a^b \in \{a, a^{-1}\}$. If $a^b = a$ then $a \in Z(G)$ (as $G = A \cup bA$), hence $a = a^{-1}$ by IV. Thus $a^b = a^{-1}$ anyway. Hence $\phi x = (\phi b)(\phi a) = b^{-1}a = a^b b^{-1} = a^{-1}b^{-1} = x^{-1}$, indeed.

VI. *If* $|G : A| > 2$ *then* A *is an elementary abelian 2-group.*

PROOF: Assume that $a^2 \neq e$ for some $a \in A$. By IV, $|C(a)| = n/2$. By III, $A \leq C(a)$, hence $|A| \leq n/4$. By II, $C(a) \cap (B \setminus a^{-1}D) = \emptyset$, hence $C(a) \subseteq A \cup D \cup a^{-1}D$. This implies $n/2 = |C(a)| \leq n/4 + 2|D| < n/2$, a contradiction, proving that $a^2 = e$.

VII. *If* $|G : A| > 2$ *then* G *is abelian but not an elementary abelian 2-group.*

PROOF: By VI, we have $\phi x = x^{-1}$ for any $x \in G \setminus D$. Now an application of Lemma 2 proves that G is abelian. If G were an elementary abelian 2-group, then $A \supseteq G \setminus D$, a contradiction.

VIII. By V and VII, the proof of Lemma 3 is complete. ■

PROOF OF THEOREM 2: Let G be a group of order n, belonging to Class II. Let d denote the minimum number of generators of G. Clearly, $d \leq [\log_2 n]$. As any automorphism of G is fully determined by its action on a generating set, we have the trivial estimate $|\mathrm{Aut}\, G| \leq (n-1)\ldots(n-d) < n^d$. Now an application of the Corollary to Lemma 1 yields a non-identity automorphism ϕ of G and a subset $D \subseteq G$ such that $\phi x \in \{x, x^{-1}\}$ for each $x \in G \setminus D$, and $|D| < 4d \log_2 n$. Hence we may apply Lemma 3, provided $4d \log_2 n \leq n/8$; in particular if $[\log_2 n] \leq n/(32 \log_2 n)$. This inequality holds for any $n \geq 4683$. Then by Lemma 3, G belongs to Class III, proving Theorem 2. ■

REFERENCES

[1] G.D. GODSIL: Neighbourhoods of transitive graphs and GGR's, preprint, University of Melbourne (1978).

[2] D. HETZEL: Graphical regular representations of cyclic extensions of small and infinite groups (to appear).

[3] W. IMRICH: Graphs with transitive Abelian automorphism groups, in: *Comb. Th. and Appl.* (P. Erdös et al. eds. Proc. Conf. Balatonfüred, Hungary 1969) North-Holland 1970, 651–656.

[4] W. IMRICH: Graphical regular representations of groups of odd order, in: *Combinatorics* (A. Hajnal and Vera T. Sós, eds.), North-Holland 1978, 611–622.

[5] M.E. WATKINS: On the action of non-abelian groups on graphs. *J. Comb. Theory (B) 1* (1971) 95–104.

[6] M.E. WATKINS: Graphical regular representations of alternating, symmetric, and miscellaneous small groups, *Aequat. Math. 11* (1974) 40–50.

[7] M.E. WATKINS: The state of the GRR problem, in: *Recent Advances in Graph Theory* (Proc. Symp. Prague 1974), Academia Praha 1975, 517–522.

(Oblatum 5–IV–1977 & 5–IX–1977)

Dept. of Algebra and Number Theory
Eötvös L. University
H-1088 Budapest
Múzeum krt. 6–8
Hungary