SMALL POSETS WITH PRESCRIBED AUTOMORPHISM GROUP

JONATHAN ARIEL BARMAK †

Abstract. We give an alternative proof of a result of Babai, that there exists a constant c such that any finite group G can be realized as the automorphism group of a poset with at most $c|G|$ points. We also provide bounds for the minimum number of points of a poset with cyclic automorphism group of a given prime power order.

1. Introduction

In 1946 Birkhoff [8] proved that if G is a finite group, then there exists a poset P of $|G|(|G|+1)$ points whose automorphism group is isomorphic to G. In 1948 Frucht [9] improved Birkhoff's bound showing that P can be taken with $|G|^2$ points. In 1950 Frucht [10] proved that P can be constructed with only $(d+2)|G|$ points if G admits a generating set of cardinality d. For generators $h_1, h_2, \ldots, h_d$, it is easy to see that the order in $G \times \{-1, 0, \ldots, d\}$ given by $(g, j) \geq (g, i)$ for $-1 \leq i \leq j$ and $(g, j) \geq (gh_i, -1)$ for $1 \leq i \leq j$, has automorphism group G. In 1980 Babai improved all previous results by showing that a poset with only $3|G|$ points can be obtained with automorphism group isomorphic to G [4, Theorem 2.1]. In [2] Babai had already proved that every finite group G different from $\mathbb{Z}_2, \mathbb{Z}_3$ and $\mathbb{Z}_5$ is the automorphism group of a graph with $2|G|$ vertices. In [4] Babai adapted his construction to classify the finite groups G which admit a *digraphical regular representation* (DRR), i.e. for some set S of generators the Cayley digraph $\Gamma(G, S)$ has automorphism group equal to G. Concretely, he describes the DRR for groups G which have a set of generators satisfying certain technical conditions. For some of the groups in the classification (cyclic, generalized dihedral, $\mathbb{Z}_3^2$ and the quaternions) the general construction does not apply and a separate argument is given. His proof uses results from [11] and [12]. Now, for any digraph Γ of n vertices there is a poset with $3n$ points and the same automorphism group [3]. Thus, any group G admiting a DRR is the automorphism group of a poset with $3|G|$ points. For a group G not having a DRR either there is a digraph realizing G with at most $|G|$ vertices or a poset of $3|G|$ points which is constructed with a different idea.

From Babai's paper the following is evident

Theorem 1. *There exists a constant k such that for any finite group G there is a poset P realizing G with at most k orbits.*

The following, however, remains open.

Conjecture 2. [6, Conjecture 4.13] *There exists a constant k such that for any finite group G there is a lattice L realizing G with at most k orbits.*

2010 *Mathematics Subject Classification.* 05E18,06A11,20B25.

Key words and phrases. Automorphism group, finite posets.

† Researcher of CONICET. Partially supported by grant PICT-2017-2806, PIP 11220170100357CO, UBACyT 20020160100081BA.

In this article we build on Babai's work in [2] to give a proof of the following

Theorem 3. *Let G be a finite group. Then there exists a poset P with $4|G|$ points whose automorphism group $Aut(P)$ is isomorphic to G. Moreover, the action of G on P is free, that is it has 4 orbits.*

Although our constant 4 is worse than Babai's 3, the advantage of our proof is that it is shorter, more direct, self-contained, and gives a general construction which works for every group G. The unique condition that we require from the generator set used in our construction is the minimality, as in [2]. The poset P we construct is not a lattice in general, but we believe it could be possible to use similar ideas to construct a lattice bigger than P which gives a direct answer to Conjecture 2.

The minimum number of vertices in a graph realizing G has been determined by Arlinghaus [1] for every abelian finite group G using results by Sabidussi and Meriwether. Meriwether solved the case G cyclic of prime power order by fixing some errors in results by Sabidussi. The analogous result for posets has not yet been settled, to the best of our knowledge. In Section 3 we prove the first general result in this context, establishing lower and upper bounds for the minimum number of points in a poset with automorphism group $\mathbb{Z}_{p^k}$.

Acknowledgement. I would like to thank Pedro Chocano Feito for drawing my attention to Babai's paper [4] after the first version of this article was completed.

2. Proof of Theorem 3

Proof. Let $H = \{h_1, h_2, \ldots, h_d\}$ be a minimal generating set of G, i.e. no proper subset generates G. By Frucht's construction of a poset with $(d+2)|G|$ points, the result holds for $d \leq 2$, so assume $d \geq 3$. We consider first the case that d is odd.

Define $h_0 = h_{-1} = e \in G$. The underlying set of P is $G \times \{0, 1, 2, 3\}$. The set of minimal points in P is $G \times \{0\}$. If $g \in G$, $(g, 1)$ covers exactly $d+1$ minimal points: all the elements of the form $(gh_{i+1}^{-1}h_i, 0)$, for $-1 \leq i \leq d-1$. The point $(g, 2)$ covers just one element, $(g, 1)$. The point $(g, 3)$ covers the points $(gh_k, 2)$ for $0 \leq k \leq d$ even and the points $(gh_k, 1)$ for $0 \leq k \leq d$ odd (see Figure 1).

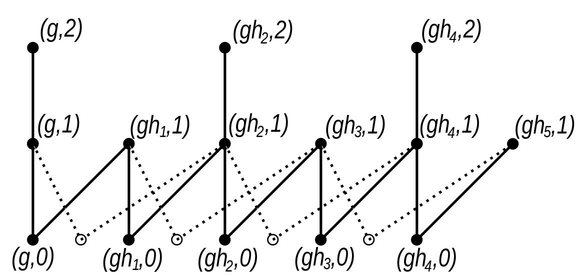

Figure 1. The subposet $P_{<(g,3)}$ for $d = 5$. There are many minimal points missing in this picture, each point of height 1 covers 6 points. The dotted lines and the empty circles represent edges and points which could be part of the poset or not, namely there could be a point smaller than $(gh_k, 1)$ and $(gh_l, 1)$ if $|k - l| = 2$, but not if $|k - l| \geq 3$.

We will say that two points $(g,1)$ and $(g',1)$ of height 1 are *adjacent* if there exists a point which is smaller than both of them. Note that $(h_k,1)$ and $(h_{k+1},1)$ are adjacent for every for every $0 \le k \le d-1$. Indeed, $h_k h_0^{-1} h_{-1} = h_k = h_{k+1} h_{k+1}^{-1} h_k$. On the other hand $(h_k,1)$ and $(h_l,1)$ are not adjacent if $|k-l| \ge 3$ $(k,l \ge 0)$. This is tedious but follows from the minimality of H. Suppose $h_k h_{i+1}^{-1} h_i = h_l h_{j+1}^{-1} h_j$. If $i=-1$, then $h_k \in \langle h_l, h_j, h_{j+1}\rangle$ and $h_l \in \langle h_k, h_j, h_{j+1}\rangle$. At least one of these contradicts the minimality of H. The same happens if $j=-1$. If $i=0$, $h_k h_1^{-1} = h_l h_{j+1}^{-1} h_j$, which contradicts again minimality. The same holds if $j=0$. If $i,j \ge 1$, without loss of generality suppose $i<j$. Then h_i must appear more than once in the expression above, so $k=i$ or $l=i$. In any case, h_{i+1} must be repeated as well, so $j=i+1$. And finally $j+1=l$ or $j+1=k$, so $|k-l|=2$, a contradiction.

Note that G acts freely on P by left multiplication on the first coordinate. This shows that G is a subgroup of $\mathrm{Aut}(P)$. The G-orbit of $(e,3)$ has size $|G|$, and since any automorphism of P maps $(e,3)$ to a maximal point, the $\mathrm{Aut}(P)$-orbit of $(e,3)$ has size at most $|G|$, so it is exactly $|G|$. In order to verify that $\mathrm{Aut}(P)$ is isomorphic to G it suffices to show that the stabilizer S of $(e,3)$ under the action of $\mathrm{Aut}(P)$ is trivial. Indeed, in that case the size of the $\mathrm{Aut}(P)$-orbit of $(e,3)$ is $|G| = |\mathrm{Aut}(P)|/|S| = |\mathrm{Aut}(P)|$ so $\mathrm{Aut}(P) \simeq G$.

Assume then that $\varphi \in \mathrm{Aut}(P)$ fixes $(e,3)$. We want to prove that φ is the identity. Since $\varphi(e,3) = (e,3)$, φ induces an automorphism of the subposet $P_{<(e,3)}$. Since φ preserves heights, $(\{e\} \cup H) \times \{1\}$ is mapped into itself. Moreover, this restriction maps adjacent points to adjacent points. If $0 \le k \le d$ is odd, then $(h_k,1)$ is maximal in $P_{<(e,3)}$, so it is mapped to another maximal point $(h_l,1)$ with l odd.

Since d is odd, $(e,1)$ is the unique non-maximal point of height 1 in $P_{<(e,3)}$ which is adjacent to exactly one maximal point: $(h_1,1)$. Indeed $(h_k,1)$ is adjacent to $(h_{k-1},1)$ and $(h_{k+1},1)$, which are maximal when k is even. Therefore $\varphi(e,1) = (e,1)$. Now, $(h_1,1)$ is the unique maximal point which is adjacent to $(e,1)$ and thus it is also fixed by φ. In general, once we have proved that $(h_l,1)$ is fixed for every $l \le k$, then $(h_{k+1},1)$ is the unique maximal or non-maximal point $(h_r,1)$ with $r \ge k+1$ which is adjacent to $(h_k,1)$ and so it is fixed as well. We deduce that φ fixes all the points of height 1 in $P_{<(e,3)}$, and it is easy to see that then it also fixes $(e,2)$. In general, if φ fixes $(g,3)$, then it fixes $(g,2)$, $(g,1)$ and moreover $(gh_k,1)$ for every $0 \le k \le d$. Conversely, if $(g,1)$ is fixed, then $(g,3)$ is fixed (if $\varphi(g,3) = (g',3)$, take $m_{g(g')^{-1}}$ the left multiplication by $g(g')^{-1}$. Then $m_{g(g')^{-1}}\varphi$ fixes $(g,3)$, so it fixes $(g,1)$, and then $g'=g$). In conclusion, $(g,3)$ fixed implies $(gh_k,3)$ fixed for every k. Since $(e,3)$ is fixed and H generates G, all the points $(g,3)$ are fixed, and then also $(g,2)$ and $(g,1)$. It only remains to prove that the points $(g,0)$ are fixed. It suffices to prove that $(e,0)$ (and then every minimal point in P) is determined by the points that cover it. Suppose $e \ne g \in G$ is such that $\{e, h_1, h_1^{-1}h_2, h_2^{-1}h_3, \dots, h_{d-1}^{-1}h_d\} = \{g, gh_1, gh_1^{-1}h_2, gh_2^{-1}h_3, \dots, gh_{d-1}^{-1}h_d\}$. Note that e and h_1 differ by a right multiplication by h_1. Now, if $i \ge 1$, $gh_i^{-1}h_{i+1}h_1 \ne gh_j^{-1}h_{j+1}$ for every $j \ge -1$, by minimality of H. And $gh_1^2 = gh_j^{-1}h_{j+1}$ only if $j=-1$ and $h_1^2 = e$. Thus, we must have $e = gh_1$, $h_1 = g$. But then $h_2 = gh_1^{-1}h_2 \in \{e, h_1, h_1^{-1}h_2, h_2^{-1}h_3, \dots, h_{d-1}^{-1}h_d\}$, which is absurd by minimality of H. This finishes the proof of the case d odd.

The case d even is very similar. The definition of P changes only for points of height 1 and 3: $P = G \times \{0,1,2,3\}$, the points $(g,0)$ are minimal. If $g \in G$, $(g,1)$ covers now d minimal points: $(g,0)$ and the points $(gh_{i+1}^{-1}h_i, 0)$, for $1 \le i \le d-1$. The point $(g,2)$ just covers $(g,1)$. The point $(g,3)$ covers $(g,2)$, the points $(gh_k,2)$ for $1 \le k \le d$ odd and the points $(gh_k,1)$ for $1 \le k \le d$ even.

As before $(h_k,1)$ and $(h_{k+1},1)$ are adjacent for $1 \le k \le d-1$, and $(h_k,1),(h_l,1)$ are non-adjacent for $k,l \ge 1$ and $|k-l| \ge 3$. Moreover, $(e,1)$ is not adjacent to $(h_k,1)$ for any $k \ge 1$. Assume $\varphi \in \mathrm{Aut}(P)$ fixes $(e,3)$. It induces a bijection on $(\{e\} \cup H) \times \{1\}$. Since $(e,1)$ is the unique point of height 1 in $P_{<(e,3)}$ which is not adjacent to any other point ($d \ge 2$), it is fixed by φ. Now, since d is even, $(h_1,1)$ is the unique non-maximal point of height 1 which is adjacent to just one maximal point, so it is also fixed. And the proof continues as in the previous case, showing that $(h_k,1)$ is fixed for every $1 \le k \le d$. Of course, $(e,2)$ is also fixed. To finish the proof we will prove that the point $(e,0)$ is determined by the set of points which cover it. Suppose $\{e, h_1^{-1}h_2, h_2^{-1}h_3, \ldots, h_{d-1}^{-1}h_d\} = \{g, gh_1^{-1}h_2, gh_2^{-1}h_3, \ldots, gh_{d-1}^{-1}h_d\}$ for some $g \neq e$. The elements e and $h_1^{-1}h_2$ differ by a right multiplication by $h_1^{-1}h_2$. But if $i \ge 2$ then $gh_i^{-1}h_{i+1}h_1^{-1}h_2 \neq gh_j^{-1}h_{j+1}$ for every $j \ge 1$ and $gh_i^{-1}h_{i+1}h_1^{-1}h_2 \neq g$, by minimality of H. On the other hand $gh_1^{-1}h_2h_1^{-1}h_2 \neq gh_j^{-1}h_{j+1}$ for every $j \ge 1$. Thus, we must have $gh_1^{-1}h_2h_1^{-1}h_2 = g$, and $g = h_1^{-1}h_2$. In particular $h_1^{-1}h_3 = gh_2^{-1}h_3 \in \{e, h_1^{-1}h_2, h_2^{-1}h_3, \ldots, h_{d-1}^{-1}h_d\}$, which is absurd, again by minimality of H. □

The proof is easier if we replace $4|G|$ by $5|G|$ in the statement, and one does not need to divide in two cases. Babai's bound $3|G|$ in general cannot be replaced by $2|G|$: $G = \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$ require $3|G|$ points at least (see next section). It would be nice to know if there is an infinite family for which the bound $2|G|$ fails.

3. Abelian groups

Example 4. If $G = \mathbb{Z}_3$ and P realizes G with minimum number of points, then there is an orbit $\mathcal{O}$ in P with 3 elements. Recall that the orbit of any group action on a finite poset is discrete (any two points are not comparable). If every other orbit has 1 element, then all the elements in $\mathcal{O}$ have the same points above and the same points below. Thus, any permutation of $\mathcal{O}$ which fixes the remaining points is an automorphism and then $|\mathrm{Aut}(P)| \ge 6$, a contradiction. There exists then a second orbit $\mathcal{O}'$ with 3 elements. Depending on the number of elements in $\mathcal{O}'$ which are comparable to each element in $\mathcal{O}$, the subposet Q of P given by these 6 points is isomorphic to one of the four posets in Figure 2.

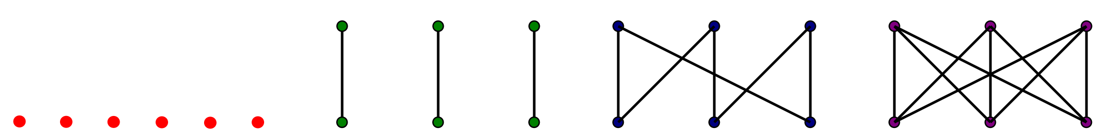

Figure 2. .

In any case, every permutation of $\mathcal{O}$ is induced by an automorphism of Q. Let $H \leqslant \mathrm{Aut}(Q)$ be the subgroup of automorphisms of Q which leave $\mathcal{O}$ invariant. Then $|H| \ge 6$. If any other orbit of the action of $\mathrm{Aut}(P)$ on P has 1 point, then the action of H on Q extends to an action on P, fixing every point not in Q. Thus $\mathrm{Aut}(P) \neq \mathbb{Z}_3$. We deduce then that there is a third orbit with 3 points, so $|P| \ge 9 = 3|G|$.

Given a finite group G denote by $\alpha(G)$ the minimum number of vertices of a graph realizing G, and by $\beta(G)$ the minimum number of points in a poset realizing G. We have just proved that $\beta(\mathbb{Z}_3) = 9$.

The number $\alpha(G)$ has been determined for all finite abelian groups by Arlinghaus [1] based on work by Sabidussi and Meriwether. The analogous result has not yet been obtained for $\beta(G)$. The computation of $\alpha(\mathbb{Z}_{p^k})$ for p prime and $k \geq 1$ is key in [1]. It is summarized in the following theorem by Meriwether.

Theorem 5. [1, Theorem 5.4]
$\alpha(\mathbb{Z}_2) = 2$.
$\alpha(\mathbb{Z}_{2^k}) = 2^k + 6$ if $k \geq 2$.
$\alpha(\mathbb{Z}_{p^k}) = p^k + 2p$ if $p = 3, 5$.
$\alpha(\mathbb{Z}_{p^k}) = p^k + p$ if $p \geq 7$ is a prime.

In this section we will prove the following

Theorem 6.
$\beta(\mathbb{Z}_2) = 2$.
$2^{k+1} \leq \beta(\mathbb{Z}_{2^k}) \leq 2^{k+1} + 12$ if $k \geq 2$.
$2p^k \leq \beta(\mathbb{Z}_{p^k}) \leq 2p^k + 3p$ if $p = 3, 5$.
$2p^k \leq \beta(\mathbb{Z}_{p^k}) \leq 2p^k + p$ if $p \geq 7$ is a prime.

Proof. The claim $\beta(\mathbb{Z}_2) = 2$ is trivial. For the other cases we prove first the lower bounds. If P is a finite poset with $\mathrm{Aut}(P) = \mathbb{Z}_{p^k}$, there must be an orbit $\mathcal{O}$ with p^k points, since otherwise every automorphism would have order dividing p^{k-1}. There must be at least one more orbit, since $\mathcal{O}$ is discrete with automorphism group S_{p^k} and $p^k > 2$. Let g be a generator of $\mathbb{Z}_{p^k}$. Suppose that all the orbits different from $\mathcal{O}$ have order smaller than p^k. Then $g^{p^{k-1}}$ fixes all the points outside $\mathcal{O}$. In particular for any $x \in \mathcal{O}$ we have $P_{<x} = P_{<g^{p^{k-1}}x}$ and $P_{>x} = P_{>g^{p^{k-1}}x}$. Thus, there is an automorphism which switches two points of P, say x_0 and $g^{p^{k-1}}x_0$, and fixes all the other. This map is different from g^i for all i, a contradiction. Thus, there is another orbit of cardinality p^k and then $|P| \geq 2p^k$.

We prove now the upper bound for $p = 3, 5$. We use in this case additive notation with $\mathbb{Z}_{p^k}$ being the integers modulo p^k. Let Q be the (crown) poset with underlying set $\mathbb{Z}_{p^k} \times \{0, 1\}$ with $(i, 1) > (i, 0) < (i + 1, 1)$ for every $i \in \mathbb{Z}_{p^k}$. Let Q' be the (subdivided crown) poset of order $3p$ and automorphism group $\mathbb{Z}_p$ constructed in [7]: $Q' = \mathbb{Z}_p \times \{0, 1, 2\}$, $(i + 1, 0) < (i, 2) > (i, 1) > (i, 0)$ for every $i \in \mathbb{Z}_p$. The underlying set of P is the disjoint union of Q and Q'. Let $q : \mathbb{Z}_{p^k} \to \mathbb{Z}_p$ be the projection. The order in P is constructed by keeping the orders within Q and Q', adding the relations $(i, 1) < (q(i), 0)$ for each $i \in \mathbb{Z}_{p^k}$ and taking the transitive closure of this relation (see Figure 3). Clearly $|P| = 2p^k + 3p$.

It is clear that $\mathbb{Z}_{p^k}$ acts faithfully on P, by left multiplication on the first coordinate (precomposing with q to act on Q'). In order to prove that $\mathrm{Aut}(P) \simeq \mathbb{Z}_{p^k}$, we only need to prove that an automorphism $\varphi : P \to P$ fixing $(0, 1) \in Q$, must be the identity. Since $(0, 0) \in Q'$ is the unique point covering $(0, 1) \in Q$, it must be fixed. Also, φ preserves heights, so it maps Q' into itself. Since $\varphi|_{Q'} : Q' \to Q'$ fixes a point, it is the identity. Now, $\varphi|_Q : Q \to Q$ is an automorphism of Q, but there are only two automorphisms fixing $(0, 1)$. One is the identity and the other maps $(i, 1) \mapsto (-i, 1)$ for every $i \in \mathbb{Z}_{p^k}$. But $(1, 0) \in Q'$ covers $(1, 1) \in Q$ and does not cover $(-1, 1) \in Q$, since $1 \neq -1 \in \mathbb{Z}_p$. Since φ fixes $(1, 0) \in Q'$, then $\varphi|_Q = 1_Q$, and we are done.

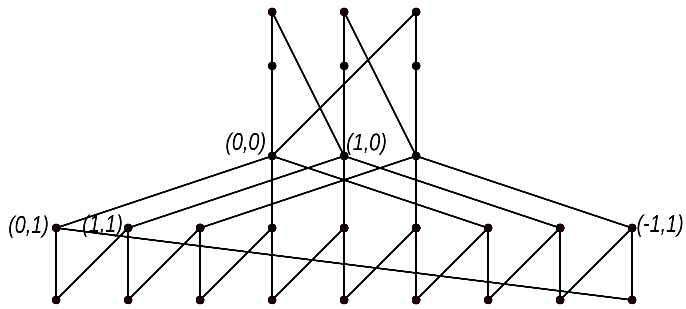

FIGURE 3. A poset P with $2p^k + 3p$ points and cyclic automorphism group of order p^k. In this case $p = 3$, $k = 2$.

For the case $p = 2, k \geq 2$, we change Q' by taking $\mathbb{Z}_4 \times \{0, 1, 2\}$ with the order defined in the same way. Since $1 \neq -1 \in \mathbb{Z}_4$ the same argument holds and $|P| = 2^{k+1} + 12$.

Finally we prove the upper bound for $p \geq 7$. We take Q as defined in the case $p = 3, 5$, but choose Q' with underlying set $\mathbb{Z}_p$ and discrete. To construct P we add the relations $(i, 1) \in Q$ is smaller than $q(i) - 1, q(i), q(i) + 2 \in Q'$ for $i \in \mathbb{Z}_{p^k}$ and take the transitive closure. We prove that an automorphism $\varphi : P \to P$ fixing $(0, 1) \in Q$ has to be the identity. Suppose φ induces the automorphism of Q which maps $(i, 1)$ to $(-i, 1)$. Since 0 covers $(0, 1)$ and $(1, 1)$, $\varphi(0)$ covers $(0, 1)$ and $(-1, 1)$, so $\varphi(0) = -1 \in \mathbb{Z}_p$. Analogously, $\varphi(-1) = 0$. Since $\{-1, 0, 2\} = P_{>(0,1)}$ is invariant, $\varphi(2) = 2$ and then the set $\{(0, 1), (2, 1), (3, 1)\}$ of points covered by 2 is invariant. But this is absurd, since $\varphi(2, 1) = (-2, 1) \neq (2, 1), (3, 1)$. Thus, $\varphi|_Q$ is the identity of Q. This implies that φ induces the identity on Q' as well, since each point in Q' is uniquely determined by the points it covers. $\square$

Problem. Improve the statement of Theorem 6: compute $\beta(G)$ for G cyclic of prime power order. More generally, for G finite cyclic and then for G finite abelian.

Babai's survey [5] of 1981 contains several results about graphs and lattices with a prescribed automorphism group. Many of these inspire questions which are open for general posets.

REFERENCES

[1] W. Arlinghaus. *The classification of minimal graphs with given abelian automorphism group.* Memoirs Amer. Math. Soc. 57 No. 330 (1985).

[2] L. Babai. *On the minimum order of graphs with groups.* Can. Bull. Math. 17(1974), pp. 467-470.

[3] L. Babai. *Infinite digraphs with given regular automorphims groups.* J. Combin. Theory Ser. B 25(1978), pp. 26-46.

[4] L. Babai. *Finite digraphs with given regular automorphisms group.* Per. Math. Hungarica 11(1980), pp. 257-270.

[5] L. Babai. *On the Abstract Group of Automorphisms.* London Math. Soc. Lecture Note Series 52, Combinatorics, Cambridge-London 1981, 1-40.

[6] L. Babai, A. Goodman. *Subdirect reducible groups and edge-minimal graphs with given automorphism group.* J. London Math. Soc. 47(1993), pp. 417-432.

[7] J.A. Barmak, E.G. Minian. *Automorphism groups of finite posets.* Discrete Math. 309(2009), pp. 3424-3426.

[8] G. Birkhoff. *Sobre los grupos de automorfismos.* Rev. Un. Mat. Argentina 11(1946), pp. 155-157.

[9] R. Frucht. *Sobre la construcción de sistemas parcialmente ordenados con grupo de automorfismos dado*. Rev. Un. Mat. Argentina, vol. 13(1948), pp. 12-18.

[10] R. Frucht. *On the construction of partially ordered systems with a given group of automorphisms*. Amer. J. Math. 72(1950), pp. 195-199.

[11] W. Imrich. *Graphs with transitive abelian automorphism group*. Combinat. Theory (Proc. Colloq., Balatonfüred, 1969), Budapest, 1970, pp. 651-656.

[12] L.A. Nowitz, M.E. Watkins. *Graphical regular representations of non-abelian groups*, I, Canad. J. Math. 24(1972), pp. 993-1008.

[13] G. Sabidussi. *On the minimum order of graphs with given automorphism group*. Monatsh. Math. 63(1959), pp. 124-127.

Universidad de Buenos Aires. Facultad de Ciencias Exactas y Naturales. Departamento de Matemática. Buenos Aires, Argentina.

CONICET-Universidad de Buenos Aires. Instituto de Investigaciones Matemáticas Luis A. Santaló (IMAS). Buenos Aires, Argentina.

E-mail address: jbarmak@dm.uba.ar