The power graph of a finite group

Peter J. Cameron[a,*], Shamik Ghosh[b]

[a]School of Mathematical Sciences, Queen Mary University of London, London E1 4NS, U.K.
[b]Department of Mathematics, Jadavpur University, Kolkata 700 032, India

Abstract

The *power graph* of a group is the graph whose vertex set is the group, two elements being adjacent if one is a power of the other. We observe that non-isomorphic finite groups may have isomorphic power graphs, but that finite abelian groups with isomorphic power graphs must be isomorphic. We conjecture that two finite groups with isomorphic power graphs have the same number of elements of each order. We also show that the only finite group whose automorphism group is the same as that of its power graph is the Klein group of order 4.

Key words: group, graph, power, isomorphism
2010 MSC: 05C25, 20D60

1. Introduction

There are a number of constructions of graphs from groups or semigroups in the literature: among these are intersection graphs of subsemigroups or subgroups (Bosák [1], Zelinka [6]), and of course Cayley graphs, which have a long history.

The *directed power graph* of a semigroup S was defined by Kelarev and Quinn [4] as the digraph $\vec{\mathcal{G}}(S)$ with vertex set S, in which there is an arc from x to y if and only if $x \neq y$ and $y = x^m$ for some positive integer m. Motivated by this, Chakrabarty *et al.* [2] defined the (undirected) power graph $\mathcal{G}(S)$, in which distinct x and y are joined if one is a power of the other. This paper concerns the general question: *what information does the power graph of S give us about S?*

An element $e \in S$ is called an *idempotent* if $e^2 = e$. If S is finite, then for each $a \in S$, there exists a natural number m such that a^m is an idempotent. Define a binary relation ρ on S by $a\rho b \Leftrightarrow a^m = b^m$ for some natural number m. Clearly ρ is an equivalence relation on S. In [2], it was shown that, for

[*] Corresponding author
Email addresses: `p.j.cameron@qmul.ac.uk` (Peter J. Cameron), `sghosh@math.jdvu.ac.in` (Shamik Ghosh)

any $a \neq b$ in S, there is a path from a to b in $\mathcal{G}(S)$ if and only if $a\rho b$. So every vertex in $\mathcal{G}(S)$ is adjacent to one and only one idempotent in S, and no two idempotents are connected by a path. Thus the components of $\mathcal{G}(S)$ are precisely the equivalence classes of ρ, and each component contains a unique idempotent to which every other vertices of that component are adjacent. In particular, $\mathcal{G}(G)$ is connected for any finite group G. Moreover in [2], it is shown that for a finite group G, $\mathcal{G}(G)$ is complete if and only if G is a cyclic group of order 1 or p^m, for some prime number p and for some natural number m.

2. The power graph of a group

In this paper we restrict our attention to groups. Two natural questions are:

- Clearly $G_1 \cong G_2$ implies $\mathcal{G}(G_1) \cong \mathcal{G}(G_2)$. Does the converse hold?
- Clearly the automorphism group of G is contained in the automorphism group of $\mathcal{G}(G)$. When does equality hold?

The answer to the first question is negative for infinite abelian groups. Let C_{p^∞} be the group of rational numbers with p-power denominators mod 1, where p is prime. Then $\mathcal{G}(C_{p^\infty})$ is a countably infinite complete graph, independent of the chosen prime.

It is false for finite groups in general. Let G be a finite group of exponent 3, that is, satisfying $x^3 = 1$ for all $x \in G$. Then $\mathcal{G}(G)$ consists of $(|G| - 1)/2$ triangles sharing a common vertex (the identity). The elementary abelian group (the direct product of cyclic groups of order 3) has exponent 3, but there are non-abelian groups as well: the smallest is the group of order 27 with presentation

$$G = \langle x, y \mid x^3 = y^3 = [x, y]^3 = 1 \rangle,$$

where $[x, y]$ is the commutator $x^{-1}y^{-1}xy$.

In fact, the phenomenon is not uncommon. A short calculation with GAP [3] and its package GRAPE [5] revealed that there are two pairs of groups of order 16 with isomorphic power graphs, and two pairs of groups of order 27. The phenomenon becomes more common; for order 32 there are one quadruple, two triples, and eight pairs.

However, we have a positive result for finite abelian groups:

Theorem 1. *Let G_1 and G_2 be finite abelian groups with $\mathcal{G}(G_1) \cong \mathcal{G}(G_2)$. Then $G_1 \cong G_2$.*

We begin the proof with the following key result. The *closed neighbourhood* of a vertex in a graph consists of the vertex and all its neighbours.

Proposition 2. *Suppose that x and y are elements of an abelian group G. Then x and y have the same closed neighbourhoods in the power graph $\mathcal{G}(G)$ if and only if one of the following holds:*

(a) $\langle x \rangle = \langle y \rangle$;

(b) G is cyclic, and one of x and y is a generator of G and the other is the identity;

(c) G is cyclic of prime power order (and x and y are arbitrary).

PROOF. It is clear that, in each of the cases (a)–(c), x and y have the same closed neighbourhoods. (If G is cyclic of prime power order, then $\mathcal{G}(G)$ is complete.) So suppose that x and y have the same closed neighbourhoods.

Without loss of generality, the order of x divides that of y; suppose these orders are k and kl respectively. Replacing x by a power of x having the same order, we may assume that $x = y^l$.

Now every element z of $\langle y\rangle$ is in the closed neighbourhood of x, and so either z is a power of x, or x is a power of z. Since there are elements of z of every order dividing kl, we see that

for each divisor m of kl, either m divides k or k divides m.

We claim that just three cases are possible:

(a) $l = 1$;

(b) $k = 1$;

(c) k and l are powers of the same prime.

For suppose that none of these conditions holds. Then at least two primes divide kl. If there is a prime p such that the power of p dividing k is positive, and a prime $q \neq p$ such that the power of q dividing l is positive, then the number $m = qk/p$ violates the displayed condition. So if p divides k, then l is a power of p, and *vice versa*; but then both k and l are powers of p, a contradiction.

In case (a) we have conclusion (a) of the theorem. We have to look at the other two cases.

Suppose that (b) holds, so that x is the identity. Then y is joined to every element of G. If G is not cyclic, then it contains two elements u, v generating distinct subgroups of some prime order p; but y cannot be joined to both u and v. So G is cyclic. If its order is not a prime power, then the only elements joined to all others are the identity and the generators. So (b) or (c) of the theorem holds.

If (c) holds, suppose that k and l are powers of p, but G is not a cyclic p-group. If the Sylow p-subgroup of G is non-cyclic, then there is an element z of order p which is not a power of y. Then $(yz)^l = x$, so x is joined to yz, but y is not. Otherwise, there is an element z of prime order $q \neq p$; then x is joined to xz, but y is not. In each case we have a contradiction.

Corollary 3. *If G is an abelian group, then $\mathcal{G}(G)$ has more than one vertex which is joined to all others if and only if G is cyclic.*

Now we can give the proof of the Theorem. The preceding Corollary shows that the Theorem is true if one of G_1 and G_2 is cyclic. So suppose not. Then the power graph of G_1 determines the equivalence relation, where two elements are equivalent if and only if they generate the same cyclic subgroup. We can recognise the identity element, as the only one joined to all others in the power graph.

Let p be the smallest prime divisor of $|G_1|$. Then the elements of order p are those lying in classes of order $p-1$. Inductively, we recognise the elements of order p^i, as those lying in classes of size $p^{i-1}(p-1)$ and having p^{i-1} neighbours among the elements of order p^{i-1} already found.

Hence we know (as a set of elements) the Sylow p-subgroup P of G_1. Knowing the numbers of elements of each order in P determines P up to isomorphism. Now the unique complement H of p consists of those elements which have no neighbour in P apart from the identity. The induced subgraph on H is $\mathcal{G}(H)$. By induction, we can determine H (and hence G_1) up to isomorphism. Clearly this shows that $G_1 \cong G_2$.

In view of the fact that Theorem 1 fails for arbitrary finite groups, we replace the first question with another:

Conjecture 1. Let G_1 and G_2 be finite groups with $\mathcal{G}(G_1) \cong \mathcal{G}(G_2)$. Then G_1 and G_2 have the same numbers of elements of each order.

This has been tested computationally for all groups of order up to 511 by John Bray; it is true in all these cases. We note that the converse fails for groups of order 16. In addition, we have the following result:

Proposition 4. *Let G_1 and G_2 be finite groups with $\vec{\mathcal{G}}(G_1) \cong \vec{\mathcal{G}}(G_2)$. Then G_1 and G_2 have the same numbers of elements of each order.*

Proof. In the directed power graph of G, the maximal complete digraphs (sets of vertices joined by arcs in both directions) are clearly the equivalence classes of the relation $\equiv$, where $x \equiv y$ if $\langle x \rangle = \langle y \rangle$. The equivalence classes are partially ordered by the relation $[y] \leq [x]$ if there is an arc from x to y. A minimal non-identity equivalence class consists of elements of prime order p, and has cardinality $p-1$. For any equivalence class $[x]$, we can now determine the set of primes dividing the order of x from the set of minimal classes below $[x]$ in the partial order. If x has order $n = p_1^{a_1} \cdots p_r^{a_r}$, we now know the primes $p_1, \ldots, p_r$ and the value of $\phi(n) = |[x]|$. The exponent a_i is one more than the exponent of the power of p_i dividing $|[x]|$. So the order of x is determined.

For the second question, we have a complete answer for finite groups.

Theorem 5. *The only finite group G for which* $\mathrm{Aut}(G) = \mathrm{Aut}(\mathcal{G}(G))$ *is the Klein group $C_2 \times C_2$.*

Proof. Let G satisfy the condition of the proposition. First note that the map $x \mapsto x^{-1}$ is always an automorphism of $\mathcal{G}(G)$, but is an automorphism of G if and only if G is abelian. So our group G is abelian.

If x is an element of order greater than 2, and y an non-identity element not in $\langle x \rangle$ whose order divides that of x, then there is a graph automorphism fixing

x and y and mapping xy to its inverse; no group automorphism can do this. We conclude that G is either cyclic or an elementary abelian 2-group.

Suppose that G is cyclic of order m. If m is composite and greater than 4, let k be a divisor of m such that $m/k > 2$. There is a graph automorphism fixing the generator x of G and mapping x^k to its inverse, which is impossible for a group automorphism. If m is a prime power, then $\mathcal{G}(G)$ is a complete graph and has an automorphism moving the identity, which no group automorphism can do.

Let G be an elementary abelian 2-group of order 2^a. Then $\mathcal{G}$ is a star $K_{1,2^a-1}$, then $\mathrm{Aut}(\mathcal{G}(G))$ is the symmetric group of degree $2^a - 1$, while $\mathrm{Aut}(G)$ is the general linear group $\mathrm{GL}(a, 2)$; these groups are equal if and only if $a = 2$.

References

[1] Juraj Bosák, The graphs of semigroups, *Theory of Graphs and Application*, Academic Press, New York (1964), 119–125.

[2] Ivy Chakrabarty, Shamik Ghosh and M. K. Sen, Undirected power graphs of semigroups, *Semigroup Forum* **78** (2009), 410–426.

[3] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. `http://www.gap-system.org`

[4] A. V. Kelarev and S. J. Quinn, Directed graph and combinatorial properties of semigroups, *J. Algebra* **251** (2002), 16–26.

[5] L. H. Soicher, The GRAPE package for GAP, Version 4.3, 2006.
`http://www.maths.qmul.ac.uk/~leonard/grape/`

[6] Bohdan Zelinka, Intersection graphs of finite abelian groups, *Czech. Math. J.* **25 (100)** (1975), 171–174.