The power graph of a finite group, II

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS, U.K.

Abstract

The directed power graph of a group G is the digraph with vertex set G, having an arc from y to x whenever x is a power of y; the undirected power graph has an edge joining x and y whenever one is a power of the other. We show that, for a finite group, the undirected power graph determines the directed power graph up to isomorphism. As a consequence, two finite groups which have isomorphic undirected power graphs have the same number of elements of each order.

Given a group G, we define the *directed power graph* $\vec{\mathcal{G}}(G)$ to be the digraph with vertex set G, having an arc $y \to x$ if x is a power of y. The *undirected power graph* $\mathcal{G}(G)$ has an undirected edge between x and y if one of them is a power of the other. These graphs have been defined and studied in [3, 4] (in the more general context of finite semigroups). The basic question is: *to what extent does the undirected or directed power graph of a group G determine G?*

The directed power graph of a group (with a loop added at each point) is a *preorder*, a reflexive transitive relation. So the relation $\approx$, defined by $x \approx y$ if $x = y$ or $x \to y$ and $y \to x$ both hold, is an equivalence relation; two elements are equivalent if they generate the same cyclic subgroup of G. The equivalence classes are partially ordered by $[x] < [y]$ if $y \to x$.

From this analysis it follows that the directed power graph carries a lot of information about the group. For example, we can recognise the identity, as the unique minimal element in the order. The elements x of prime order are those lying in classes $[x]$ covering the identity (where a covers b if $b < a$ but there is no c satisfying $b < c < a$); the order of such an element x is $|[x]| + 1$. Now, if y is an element of finite order, we can determine the prime divisors of the order of y by looking at the classes covering $[1]$ and lying below y; then we can determine the order of y, since if the order of y is $p_1^{a_1} p_2^{a_2} \cdots$, then

$$|[y]| = (p_1 - 1)p_1^{a_1-1}(p_2 - 1)p_1^{a_2-1} \cdots .$$

On the other hand, if y has infinite order, then there are no elements below $[y]$ which cover $[1]$. In other words, we have:

Proposition 1 *Two groups having isomorphic directed power graphs have the same numbers of elements of each order (finite or infinite); indeed, an isomorphism between directed power graphs preserves orders of elements.*

It is not the case that two finite groups with isomorphic power graphs must themselves be isomorphic. For example, let G be a group of exponent 3. Then, in the directed power graph of G, we have $x \to 1$ for all x, and $x \to x^2$ and $x^2 \to x$ for all $x \neq 1$; there are no other edges. So the graph consists of a number of triangles with a common vertex, the edges containing this vertex directed towards it and the remaining edges being undirected. So groups of exponent 3 with the same order have isomorphic directed power graphs. Of course, such groups need not be isomorphic. For example, the elementary abelian group of order 27, and the non-abelian group

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

have isomorphic directed power graphs.

Also, the converse of Proposition 1 is false; there are groups with the same numbers of elements of each order whose directed power graphs are not isomorphic. However, a finite abelian group is determined up to isomorphism by its power graph [2]. Even this fails for infinite groups: the power graph of the Prüfer group C_{p^∞} is a countable complete graph, for any prime p.

At the British Combinatorial Conference in 2009, Shamik Ghosh asked a question about undirected power graphs, which, after discussion with the author of this paper, became the following: *is it true that two finite groups with isomorphic undirected power graphs have the same numbers of elements of each order?* Here, I answer this question in the affirmative. In fact, I prove the following theorem:

Theorem 2 *If G_1 and G_2 are finite groups whose undirected power graphs are isomorphic, then their directed power graphs are also isomorphic.*

Corollary 3 *Two finite groups whose undirected power graphs are isomorphic have the same numbers of elements of each order.*

The corollary follows immediately from the Theorem and Proposition 1. Before embarking on the proof of the main theorem, I show the following result.

Proposition 4 *Let G be a finite group; let S be the set of vertices of the power graph $\mathcal{G}(G)$ which are joined to all other vertices. Suppose that $|S| > 1$. Then one of the following occurs:*

(a) G is cyclic of prime power order, and $S = G$;

(b) G is cyclic of non-prime-power order n, and S consists of the identity and the generators of G, so that $|S| = 1 + \phi(n)$;

(c) G is generalised quaternion, and S contains the identity and the unique involution in G, so that $|S| = 2$.

Proof Take $g \in S$ with $g \neq 1$. First I claim that the order of g is divisible by every prime divisor of $|G|$. For if q is a prime dividing $|G|$ but not $o(g)$, and h an element of order q, then clearly h is not joined to g in the power graph.

Suppose first that G is a p-group, for some prime p. Some power of g has order p. Now G has a unique subgroup of order p; for if h is an element of order p which is not a power of g, then h is not joined to g in the power graph. Now a p-group with a unique subgroup of order p is cyclic or generalised quaternion, by [1, Theorems 8.5, 8.6]. In these cases we obtain conclusions (a) or (c) of the Proposition.

So suppose that the order of G is divisible by at least two distinct primes. Then every element of prime order is a power of g, so G contains a unique subgroup of order p for every prime p dividing $|G|$. This implies that G is cyclic. Then g must generate G, since in a cyclic group of non-prime-power order, every non-identity non-generator has a non-neighbour in the power graph.

Now for each of these groups, we can recognise the group from its power graph. If G is cyclic of prime-power order, then $\mathcal{G}(G)$ is the complete graph; if G is cyclic of non-prime-power order n, then $\mathcal{G}(G)$ has $1+\phi(n)$ vertices joined to all others; and if G is generalised quaternion, then it has just two such vertices.

So for the rest of the proof of Theorem 2, we can assume that G is neither cyclic nor generalised quaternion; then we can recognise the identity as the only vertex joined to all others. Let $X=\mathcal{G}(G)$ be the undirected power graph of such a group G.

Let $\bar{N}(x)$ denote the closed neighbourhood of x, and define an equivalence relation on G by the rule that $x \equiv y$ if $\bar{N}(x)=\bar{N}(y)$. Note that the following conditions for two elements x and y of the same order are equivalent:

(a) x is joined to y in the power graph;

(b) $x \equiv y$;

(c) $\langle x\rangle = \langle y\rangle$ (that is, $x \approx y$).

For if (a) holds, then $y=x^k$, where k is coprime to the order m of x; so also x is a power of y, which implies (b) and (c). Conversely, each of (b) and (c) clearly implies (a).

So the relation $\approx$ is a refinement of $\equiv$, and our main task is to investigate how these relations may differ.

Proposition 5 *Each non-identity $\equiv$-class C is of one of the following forms:*

(a) C is a $\approx$-class;

(b) y is an element of order p^r for some prime p, and $C=\{x\in\langle y\rangle : o(x) > p^s\}$ for some $s<r-1$, so that C is the union of $r-s$ $\approx$-classes.

Proof We've seen that (a) holds if all elements of C have the same order.

Suppose that $x\equiv y$ and $o(x)<o(y)$. Then x and y are joined, so x is a power of y. We show first that $o(y)$ is a prime power. Every element $z\in A=\langle y\rangle$ is in the closed neighbourhood of y, and hence that of x; so either x is a power of z, or z a power of x.

Let $o(x)=k$ and $o(y)=kl$. Replacing y by a power if necessary, we can assume that $x=y^l$. Let p be a prime dividing k. If l is divisible by a prime $q\neq p$, then there is an element of A of order kq/p, which cannot be joined to

x. So if p divides k, then l is a power of p. The same conclusion holds with k and l reversed. So it must be that k and l are powers of the same prime.

Now let x and y be elements whose orders are powers of a prime p. Then $\bar{N}(x) \supseteq \bar{N}(y)$ if and only if x is a power of y. For the forward implication is clear since $\bar{N}(x) \supseteq \bar{N}(y)$ implies that x and y are joined in the power graph. So suppose that x is a power of y, and take $z \in \bar{N}(y)$. If y is a power of z, then so is x; if z is a power of y, then x and z both lie in the cyclic p-group generated by y, and the power graph of a cyclic p-group is a complete graph. So $z \in \bar{N}(x)$ in either case.

So, if C is a $\equiv$-class containing elements of different orders, then all elements of C have orders which are powers of a prime p. Take elements x and y of minimal and maximal orders in C, say p^{s+1} and p^r, with $s < r$; then every power of y whose order is greater than p^s belongs to C, and conclusion (b) holds.

Now I claim that we can recognise a class of type (b) and reconstruct the corresponding prime p from the graph structure.

For any set S, let $\bar{N}(S) = \bigcap\{\bar{N}(v) : v \in S\}$, and let $\hat{S} = \bar{N}(\bar{N}(S))$. We show that, if C is a class of type (b), then $|\hat{C}| = p^r$ for some prime p and positive integer r, and $|C| = p^r - p^s$ for some $s < r - 1$.

We know that $\langle C \rangle = A$ is a cyclic group, and $\bar{N}(a) \supseteq \bar{N}(c)$ for any $a \in A$, $c \in C$. Hence $A \subseteq \hat{C}$. We show that equality holds. Suppose that $u \in \hat{C} \setminus A$. We consider two cases:

- The order of u is not a power of p, say $o(u) = p^{r+t}m$ where p does not divide m. Then $u^{p^{t+1}}$ is adjacent to y^p (where y is an element of order p^r in C), but not to y, contradicting the fact that $y \equiv y^p$.

- The order of u is a power of p. Then $\bar{N}(u) \subsetneq \bar{N}(y)$, for $y \in C$, and the containment is proper since $u \notin C$; so $u \notin \hat{C}$, a contradiction.

This proves the assertion.

Next we have to show that a class of type (a) cannot satisfy these conditions. Let C be such a class. Note that $\hat{C}$ is a union of $\equiv$-classes. The conditions that $|\hat{C}| = p^r$ and $|C| = p^r - p^s$ imply that $|\hat{C}| \leq 2|C|$. Moreover, $1 \in \hat{C}$, so any other class in $\hat{C}$ must be strictly smaller than C. We distinguish two cases:

- C consists of elements of prime power order, say q^t. No class of elements of larger order can occur in C (such classes would be too large), so $\hat{C}$

consists of C together with classes whose orders are smaller powers of q. Then $|\hat{C}|$ can only be a prime power if $|\hat{C}| = q^t$. But then $p = q$, $r = t$, and $|C| = p^r - p^{r-1}$ contradicts the second part of (b).

- C consists of elements of non-prime-power order m. Apart from $C \cup \{1\}$, no powers of elements of C can lie in $\hat{C}$, since for any non-identity non-generator of a cyclic group of order m, there is an element not joined to it in the power graph. As before, there cannot be any classes of elements of larger order in $\hat{C}$. So $|\hat{C}| = |C| + 1$, which again violates the second part pf (b).

It follows that we can recognise equivalence classes of type (b) and reconstruct the numbers of elements of each possible order in such classes from the power graph.

Proof of Theorem 2 First note that the elements of a $\equiv$-class are indistinguishable: they can be permuted arbitrarily by graph automorphisms fixing all other vertices. Also, as noted, we can recognise classes of type (b). For such a class, of size $p^r - p^s$, partition it into subsets of sizes $p^i - p^{i-1}$ for $i = s+1, \ldots, r$ arbitrarily. Now, up to graph isomorphism, we have partitioned the vertices into equivalence classes of the relation $\approx$.

In the directed power graph, vertices in the same $\approx$-class are joined by arcs in both directions, while between different classes we have either all arcs in one direction, or no arcs at all. So we only have to assign directions to the edges between $\approx$-classes. Now a $\approx$-class has size $\phi(n)$, where n is the order of its elements; and, if $m \mid n$, then $\phi(m) \mid \phi(n)$, with equality only if $m = n$ or m is odd and $n = 2m$. So, if two classes of different sizes are joined, we direct the edges from the larger class to the smaller; and if two classes of the same size are joined, then one but not the other is also joined to an involution (a non-identity singleton class); we direct the edges from this class to the other one.

References

[1] W. Burnside, *Theory of Groups of Finite Order*, Dover Publ. (reprint), New York, 1955.

[2] Peter J. Cameron and Shamik Ghosh, The power graph of a finite group, preprint.

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

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