Power graphs of finite groups

Eilidh McKemmie
supervised by Peter M. Neumann

This was submitted as a Part B Mathematical Extended Essay
for FHS Mathematics and Computer Science
Oxford University, Hilary Term 2014
Abstract

We describe the power graphs of some well-known finite groups, and take a step towards describing the power graph of any finite abelian group. We discuss the graph theoretical properties of power graphs of finite groups, and give necessary and sufficient conditions for planarity and for the existence of an Euler trail. Cameron and Ghosh [5] list the finite groups which have the same automorphism group as their undirected power graph, and we give a similar result for the directed case. Finally, we discuss what the power graph of a finite group tells us about the group.

Notes

Because of the large volume of papers which were published while I was writing this essay, I have not taken account of any work published after 31 December 2013. Results which are not referenced are my own work. I used GeoGebra ([12]) to create all of the figures in this essay.

Acknowledgements

I would like to thank my supervisor Peter M. Neumann for his guidance, support and enthusiasm, and Colin McDiarmid for suggesting this topic to me.
Contents

1 Introduction ............................... 1

2 Describing power graphs of particular finite groups ................. 1
   2.1 Cyclic groups ........................................ 1
   2.2 Dihedral groups ..................................... 6
   2.3 Dicyclic groups .................................... 6
   2.4 Abelian groups .................................... 7

3 Graph theoretic properties of power graphs ......................... 9
   3.1 Connectivity .......................................... 9
   3.2 Total valency ......................................... 11
   3.3 Planarity ............................................. 12
   3.4 Euler circuits and trails ............................ 14

4 The automorphism group of a power graph ........................ 16

5 How much information about a group does its power graph carry? 18
1 Introduction

Kelarev and Quinn [13] define the directed power graph \( \tilde{g}(G) \) of the group \( G \) to be the graph whose vertex set is the group, with an edge from \( x \) to \( y \) whenever \( x \neq y \) and \( \langle y \rangle \leq \langle x \rangle \). Chakrabarty, Ghosh and Sen [6] then define the undirected power graph \( g(G) \) of the group \( G \) as the graph whose vertex set is the group, with two vertices \( x \neq y \) adjacent whenever \( \langle y \rangle \leq \langle x \rangle \) or \( \langle x \rangle \leq \langle y \rangle \), that is, the underlying undirected graph of the directed power graph. The restricted power graph \( g^*(G, S) \) of a group \( G \) and a subset \( S \subseteq G \) of the elements in \( G \) is the undirected power graph \( g(G) \) with the vertices in \( S \) removed. For simplicity, we write \( g^*(G) \) for the graph \( g^*(G, \{e\}) \), the undirected power graph with the identity removed. We define \( \tilde{g}^*(G) \) analogously as the graph \( \tilde{g}(G) \) with the identity removed.

Throughout this essay, we will assume that \( 0 \notin \mathbb{N} \), and that groups are multiplicative with identity \( e \), apart from the cyclic group of order \( n \) which we prefer to think of as the additive group of integers modulo \( n \), denoted \( \mathbb{Z}_n \), with identity 0. We also define Euler’s totient function.

**Definition 1.1.** Euler’s totient function \( \phi \) is defined for \( n \in \mathbb{N} \) as \( \phi(n) = |\{k \in \mathbb{N} \mid k < n, \text{hcf}(k, n) = 1\}| = |(\mathbb{Z}_n)^*| \) where \((\mathbb{Z}_n)^*\) is the multiplicative group of integers modulo \( n \). Note also that \( \phi(d) \) is the number of elements of order \( d \) in \( \mathbb{Z}_n \) for every \( d \) which divides \( n \).

2 Describing power graphs of particular finite groups

Describing the power graphs of some well-known groups is useful for building an intuition for what power graphs look like. We begin with some definitions to help us describe graphs.

**Definition 2.1.** \( K_n \) is the complete undirected graph on \( n \) vertices, that is, the graph with \( n \) vertices and an edge between every pair of distinct vertices.

\( K_{m,n} \) is a complete bipartite graph with a vertex set that can be partitioned into two disjoint sets sized \( m \) and \( n \) respectively, with an edge between two vertices if and only if they are in different parts.

**Definition 2.2.** The union \( \Gamma_1 \cup \Gamma_2 \) of two graphs \( \Gamma_1 = (V_1, E_1) \) and \( \Gamma_2 = (V_2, E_2) \) is the graph whose vertex set is \( V_1 \cup V_2 \) and whose edge set is \( E_1 \cup E_2 \). We will write \( m\Gamma \) for the union of \( m \) disjoint copies of \( \Gamma \).

The join \( \Gamma_1 + \Gamma_2 \) of two graphs \( \Gamma_1 \) and \( \Gamma_2 \) is the graph whose vertex set is \( V_1 \cup V_2 \) and whose edge set is \( E_1 \cup E_2 \cup (V_1 \times V_2) \). That is, \( \Gamma_1 \cup \Gamma_2 \) together with all the edges joining elements in \( V_1 \) with elements in \( V_2 \).

We note that, for any subgroup \( H \) of a group \( G \), \( g(H) \) is an induced subgraph of \( g(G) \) [6, Proposition 4.5]. This is obvious from the definition.

2.1 Cyclic groups


**Theorem 2.1.** For a finite group \( G \), \( g(G) \) is complete if and only if \( G \) is the cyclic group of order \( p^m \) for some prime \( p \) and non-negative integer \( m \) [6, Theorem 2.12].

**Proof.** Assume \( G \) is the cyclic group of order \( p^m \). We will show by induction on \( m \) that \( g(G) \cong K_{p^m} \).

In the base case \( m = 0 \), \( G \) is the trivial group, so \( g(G) \cong K_1 \), the complete graph on one vertex.

Now suppose that \( m > 0 \). Viewing \( G \) as \( \mathbb{Z}_{p^m} \), the additive group of integers modulo \( p^m \), and letting \( H = \{p, 2p, \ldots, p^{m-1}p\} \), we see that the generators of \( G \) are exactly the elements of \( G \setminus H \). So all of the elements in \( G \setminus H \) are adjacent to all elements of \( G \) in \( g(G) \). Now \( H \cong \mathbb{Z}_{p^{m-1}} \),
so by the induction hypothesis, \( g(H) \cong K_{p^{m-1}} \), and so the elements of \( H \) are adjacent to all the elements of \( H \) and all the elements of \( G \setminus H \) in \( g(G) \). Therefore, \( g(G) \cong K_{p^m} \).

For the converse, we take cases for \( G \).

Case \( G \) is not cyclic: Every finite group has a finite set of generators (obviously since the group generates itself). Take a minimal set \( \{\alpha_1, \ldots, \alpha_n\} \) of generators of \( G \) such that \( \langle \alpha_1, \ldots, \alpha_n \rangle = G \) and \( \alpha_i \notin \langle \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n \rangle \) for \( i = 1, 2, \ldots, n \). Since \( G \) is not cyclic, we have \( n > 1 \), and so for all pairs \( \alpha_i \neq \alpha_j \), there is no edge between \( \alpha_i \) and \( \alpha_j \) in the graph \( g(G) \), so \( g(G) \) is not complete.

Case \( G \) is cyclic with order \( n \) where \( n \) has at least two distinct prime divisors: Let \( n = pqk \) for \( k \in \mathbb{N} \) and distinct primes \( p \) and \( q \). We look at the elements \( pk \) and \( qk \) of \( G \cong \mathbb{Z}_{pqk} \), which have orders \( q \) and \( p \) respectively. We see that \( pk \) and \( qk \) are not adjacent in \( g(G) \) because \( qk \notin \langle pk \rangle = \{pk, 2pk, \ldots, qpqk = n\} \) and \( pk \notin \langle qk \rangle = \{qk, 2qk, \ldots, pqk = n\} \). So \( g(G) \) is not complete.

So if \( g(G) \) is complete, \( G \) is a cyclic group of order \( n \) where \( n \) can have at most one prime divisor, that is, \( n = 1 \) or \( p^m \) for some prime \( p \) and \( m \in \mathbb{N} \).

Chelvam and Sattanathan [8] characterise power graphs of groups of order \( pq \) for distinct primes \( p \) and \( q \).

**Theorem 2.2.** For \( G \) a finite group of order \( pq \) where \( p > q \) are distinct primes,

1. \( G \) is cyclic if and only if \( g(G) \cong (K_{p-1} \cup K_{q-1}) + K_{\phi(pq)+1} \).
2. \( G \) is not cyclic if and only if \( g(G) \cong K_1 + (pK_{q-1} \cup K_{p-1}) \).

[8, Theorem 5].

The proof in [8] uses Sylow's Theorem, but it is not necessary, so we give a proof without it here.

**Proof.** (i) Let \( G \cong \mathbb{Z}_{pq} \). Since \( \mathbb{Z}_p \times \mathbb{Z}_q \) has an element \( (1,1) \) of order \( pq \), \( G \cong \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q \). Now \( G \) has an identity and \( \phi(m) \) elements of order \( m \) for \( m = p, q, pq \). The elements of order \( p \) form a cyclic group \( \langle (1,0) \rangle \) of order \( p \) with the identity element. Similarly, the elements of order \( q \) form a cyclic group \( \langle (0,1) \rangle \) of order \( q \) with the identity element. Since \( \langle (1,0) \rangle \cap \langle (0,1) \rangle = \{(0,0)\} \), \( g(G) \) contains one copy of \( K_p \) and one copy of \( K_q \) which share only the identity vertex. Now only the elements of order \( pq \) and the identity element remain. There are \( \phi(pq)+1 \) of these and they are adjacent to every vertex in the graph. Therefore, we get that \( g(G) \cong (K_{p-1} \cup K_{q-1}) + K_{\phi(pq)+1} \).

Conversely, let \( g(G) \cong (K_{p-1} \cup K_{p-1}) + K_{\phi(pq)+1} \). Then \( |G| = (p-1) + (q-1) + \phi(pq) + 1 = (p-1) + (q-1) + (pq - p - q + 1) + 1 = pq \). There are \( \phi(pq)+1 \) elements which are adjacent to every element in the graph, one of which is the identity. But \( \phi(pq) \geq 1 \), and so there is at least one non-identity element adjacent to all other elements. This element must have order \( p \), \( q \) or \( pq \). If it has order \( p \), it cannot generate an element of order \( q \). Similarly, an element of order \( q \) cannot generate an element in order \( p \). This means that the element has order \( pq \). Since \( G \) is a group of order \( pq \) with an element of order \( pq \), it must be cyclic.

(ii) \( g(G) \cong K_1 + (pK_{q-1} \cup K_{p-1}) \) has exactly one element adjacent to all the rest. This must be the identity element, so there is no element which generates the whole group by itself, hence \( G \) is not cyclic.

Conversely, if \( G \) is a group of order \( pq \) which is not cyclic, then there are no elements of order \( pq \). This means all the non-identity elements have order \( p \) or \( q \). Say that there are two elements \( x, y \in G \) of order \( p \) such that \( \langle x \rangle \neq \langle y \rangle \). Let \( X = \langle x \rangle \) and \( Y = \langle y \rangle \), and define \( XY = \{ab \mid a \in X, b \in Y\} \). Then, since \( X \) and \( Y \) are subgroups of \( G \), we know from B2b Group Theory and an Introduction to Character Theory that \( |XY| = \frac{|X||Y|}{|X \cap Y|} \). Since \( \langle x \rangle \neq \langle y \rangle \), we know \( X \cap Y = \{e\} \), so \( |XY| = |X||Y| = p^2 \), but by definition, \( XY \subseteq G \). So we have a contradiction since \( |G| = pq < p^2 \).

This means that all elements of order \( p \) in \( G \) generate the same cyclic subgroup, so there are \( p-1 \) elements of \( G \) of order \( p \). The remaining elements are the identity and the elements of
order \( q \), so there are \( pq - p = p(q - 1) \) elements of order \( q \) in \( G \). Hence, the elements of \( G \) fall into \( p \) cyclic subgroups of \( G \) of order \( q \) and one of order \( p \), all of which share only the identity element. Therefore, we get \( p \) distinct copies of \( K_{q-1} \) and a copy of \( K_{p-1} \) all joined to one copy of \( K_1 \) for the power graph of \( G \). So \( g(G) \cong K_1 + (pK_{q-1} \cup K_{p-1}) \). 

To achieve a more general result for finite cyclic groups of any order, we must first prepare the ground by defining the graph \( A_r \) for some integer \( r \).

\[
A_r = \begin{cases} 
K_{r-1} & \text{if } r \text{ is a prime or 1} \\
K_{\phi(r)} + \left( \bigcup_{i=1}^{\phi(r)} A_{\frac{r}{\phi(r)}} \right) & \text{if } r = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \text{ for } k \geq 1, \text{ distinct primes } p_i, \text{ and } m_i \in \mathbb{N}.
\end{cases}
\]

Now we will use these graphs to construct the power graph of any cyclic group. We cannot write this in terms of joins and unions of complete graphs because parts of these subgraphs overlap. Therefore we write a formula in terms of graphs \( A_r \) in which every occurrence of \( A_r \) refers to the same graph \( A_r \), not another copy of \( A_r \).

**Theorem 2.3.** For \( n = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \) where \( p_1, \ldots, p_k \) are distinct primes and \( m_1, \ldots, m_k \) are positive integers, \( g(\mathbb{Z}_n) \cong K_{\phi(n)+1} + \left( \bigcup_{i=1}^{k} A_{\frac{n}{\phi(n)}} \right) \).

**Proof.** We define

\[
D_r = \{a_1^{\alpha_1}a_2^{\alpha_2} \cdots a_r^{\alpha_r} | 1 \leq i_1 < \cdots < i_r \leq k, 0 < a_{ij} \leq m_{ij} \text{ for } j = 1, \ldots, r\}
\]

for \( 1 \leq r \leq k \), and note that the divisors of \( n \) (excluding 1) are exactly the elements of the disjoint union \( D = \bigcup_{r=1}^{k} D_r \). We construct the power graph \( g(G) \) in rounds, in the \( r \)th round adding every element whose order is in \( D_r \) in increasing order, and adding all its out-edges to elements which are already in the graph. Because of the order in which we add the elements, we never need to backtrack to add an in-edge to a vertex \( x \in \mathbb{Z}_n \) which we are adding, since if \( a \in \langle x \rangle \) then either we have already added a vertex for \( a \) to our graph, or \( x \in \langle a \rangle \) so we add the edge between \( a \) and \( x \) when we add the vertex \( a \). So we have ensured that we have all of the vertices and edges of \( g(\mathbb{Z}_n) \) in the graph we are constructing, and no other vertices or edges.

We show by induction on \( r \) that, for \( r = 1, \ldots, k-1 \), after the \( r \)th round, we have the graph

\[
\bigcup_{1 \leq i_1 < \cdots < i_r \leq k, 0 < a_{ij} \leq m_{ij}} A_{p_{i_1}^{a_{i_1}}p_{i_2}^{a_{i_2}} \cdots p_{i_r}^{a_{i_r}}} = \bigcup_{1 \leq i_1 < \cdots < i_r \leq k} A_{p_{i_1}^{m_{i_1}}p_{i_2}^{m_{i_2}} \cdots p_{i_r}^{m_{i_r}}}.
\]

The equality holds by the definition of \( A_r \) which says that each graph \( A_{p_{i_1}^{a_{i_1}}p_{i_2}^{a_{i_2}} \cdots p_{i_r}^{a_{i_r}}} \) for \( a_{ij} \leq m_{ij} \) is a subgraph of \( A_{p_{i_1}^{m_{i_1}}p_{i_2}^{m_{i_2}} \cdots p_{i_r}^{m_{i_r}}} \). So we will show that, after the \( r \)th round, the graph we have constructed is the union of the graphs \( A_i \) where \( i \) is a product of exactly \( r \) elements of \( \{p_1^{a_{i_1}}, \ldots, p_k^{a_{i_k}}\} \).

**Round 1** (base case): For fixed \( i \) such that \( 1 \leq i \leq k \), all the elements of order \( p_i \), of which there are \( p_i - 1 \), generate the same cyclic subgroup of order \( p_i \). We do not add the identity yet, so we have a copy of \( \mathbb{Z}_{p_i}^* \cong K_{p_i-1} \). We call this graph \( A_{p_i} \). Adding the elements of order \( p_i^2 \) means joining to \( A_{p_i} \) a copy of \( \mathbb{Z}_{p_i^2}^* \cong K_{\phi(p_i^2)} \), the power graph of a cyclic group of order \( p_i^2 \) without its cyclic subgroup of order \( p_i \). So, having added all the elements of order \( p_i^2 \), we have the graph \( A_{p_i^2} \). We continue adding elements of order \( p_i^l \) for \( l = 1, \ldots, m_i \), and get the graph \( A_{p_i^{m_i}} \) for this fixed value of \( i \).

Now if we let \( i \) vary, the graphs \( A_{p_i^{m_i}} \) are disjoint. After round 1, we have the graph

\[
\bigcup_{i=1}^{k} A_{p_i^{m_i}},
\]

as required.

**Round \( r \)** (inductive step): By the induction hypothesis, at the end of round \( r-1 \) we have the graph

\[
\Gamma = \bigcup_{1 \leq i_1 < \cdots < i_{r-1} \leq k} A_{p_{i_1}^{m_{i_1}}p_{i_2}^{m_{i_2}} \cdots p_{i_{r-1}}^{m_{i_{r-1}}}}.
\]
In round $r$, we add all the elements whose order is a product of exactly $r$ powers of the distinct primes $p_1, \ldots, p_k$ in increasing order. Fix $i_1 < \cdots < i_r$ and $a_{i_j} \leq m_j$ for $j = 1, \ldots, r$ and let $m = p_{i_1}^{a_{i_1}} \cdots p_{i_r}^{a_{i_r}}$. To simplify notation, let $b_j = p_{i_j}^{m_j}$ for all $j$.

There are exactly $\phi(m)$ elements of order $m$ in $G$, and they all generate the same cyclic subgroup of $G$. This cyclic group is made up of the elements of order $m$ and all those in cyclic subgroups of order $\frac{m}{q_j}$ for $j = 1, \ldots, r$ where $q_j$ divides $b_j$. We have already added the elements whose order divides $\frac{m}{q_j}$ for $j = 1, \ldots, r$ in the previous round, and because we add elements in increasing order during this round, we have already added the elements in cyclic subgroups of order $\frac{m}{q_j}$ for $j = 1, \ldots, r$ where $q_j$ divides $b_j$, which are represented in the graphs $A_{\frac{m}{q_j}}$. So we create a copy of $K_{\phi(m)}$ which contains the elements of order $m$ and join it to the graph

$$\Gamma' = \bigcup_{1 \leq i_1 < \cdots < i_r \leq k, \ q_j | b_j} A_{\frac{m}{q_j}}.$$

In doing so, we create the graph $K_{\phi(m)} + \Gamma'$, which contains $\Gamma$ and $A_m$. We do this for each $m$ which is a product of exactly $r$ powers of the distinct primes $p_1, \ldots, p_k$. In the end, we have a union of the $A_m$ graphs, which means we have the graph

$$\bigcup_{1 \leq i_1 < \cdots < i_r \leq k} A_{p_{i_1}^{m_{i_1}} p_{i_2}^{m_{i_2}} \cdots p_{i_r}^{m_{i_r}}}.$$

In the last round, we must add the elements of order $n$, which generate the group $G$, so all we need to do is add a copy of $K_{\phi(n)}$ to our graph

$$\bigcup_{1 \leq i_1 < \cdots < i_r \leq k} A_{p_{i_1}^{m_{i_1}} p_{i_2}^{m_{i_2}} \cdots p_{i_r}^{m_{i_r}}} = \bigcup_{i=1}^{k} A_{\frac{n}{p_i}}.$$

We then add the identity element, which gives us that $g(G) \cong K_{\phi(n)} + 1 + \left( \bigcup_{i=1}^{k} A_{\frac{n}{p_i}} \right)$. 

**Example 2.1.** Together, Figures 1, 2, and 3 show how $g(Z_{12})$ is built in this way.
Figure 1: Round 1: start with elements 6 (order 2, in blue), 4 and 8 (order 3, in green), and 3 and 9 (order 4, in red) to get $A_4 \cup A_3$

Figure 2: Round 2: add elements 2 and 10 (of order 6, in pink) to get $A_6 \cup A_4$

Figure 3: Finally add elements of order 12 (in orange) and the identity (in black) to get $\mathfrak{g}(\mathbb{Z}_n) \cong K_5 + (A_6 \cup A_4)$
2.2 Dihedral groups

Definition 2.3. The dihedral group of order $2n$ is

$$D_{2n} = \langle \sigma, \rho \mid \rho \sigma = \sigma^{-1} \rho, \text{ord}(\sigma) = n, \text{ord}(\rho) = 2 \rangle.$$ 

Chattopadhyay and Panigrahi \cite{6} characterise power graphs of dihedral groups.

Proposition 2.1 (\cite{6}). For $n \geq 3$, $g(D_{2n}) \cong (g^*(\mathbb{Z}_n) \cup nK_1) + K_1$. See Figure 4.

Proof. The elements of $\langle \sigma \rangle \leq D_{2n}$ induce in $g(D_{2n})$ the graph $g(\langle \sigma \rangle) \cong g(\mathbb{Z}_n)$. The remaining elements of $D_{2n}$ are elements of the form $\rho \sigma^i$ for $i = 1, \ldots, n$. Note that $(\rho \sigma)^2 = (\rho \sigma)(\rho \sigma) = \rho \sigma \sigma^{-1} \rho = \rho^2 = e$. We use this as the base case for an inductive argument that $\rho \sigma^i$ has order 2 for $i = 1, 2, \ldots, n$:

$$(\rho \sigma^i)^2 = (\rho \sigma^i)(\rho \sigma^i) = (\rho \sigma^{i-1} \sigma)(\sigma^{-1} \rho \sigma^{i-1}) = (\rho \sigma^{i-1})(\rho \sigma^{i-1}) = (\rho \sigma^{i-1})^2 = e$$

by the inductive hypothesis.

So $\rho, \rho \sigma, \ldots, \rho \sigma^{n-1}$ are all adjacent only to the identity vertex in $g(D_{2n})$, giving $g(D_{2n}) \cong (g^*(\mathbb{Z}_n) \cup nK_1) + K_1$. \hfill \Box

2.3 Dicyclic groups

Definition 2.4. The dicyclic group of order $4n$ is $Q_{4n} = \langle a, b \mid a^{2n} = e, a^n = b^2, ab = ba^{-1} \rangle$.

The generalised quaternion group of order $2^k$ for $k \geq 2$ is $Q_{2^k}$.

Chattopadhyay and Panigrahi \cite{6} characterise power graphs of dicyclic groups.

Proposition 2.2 (\cite{6}). For $n \geq 2$, $g(Q_{4n}) \cong g(\langle a \rangle) \cup n(A + K_2)$ where $A$ is the subgraph of $g(\langle a \rangle)$ induced by $\{e, a^n\}$, and every mention of $A$ (including the implicit mention of $A$ contained within $g(\langle a \rangle)$) refers to the same graph. See Figure 5.
Proof. The elements of \( \langle a \rangle \leq Q_{4n} \) form a copy of \( g(\langle a \rangle) \cong g(\mathbb{Z}_{2n}) \). The remaining elements of \( Q_{4n} \) are the elements \( a^ib \) for \( i = 0, \ldots, 2n-1 \). We use the fact that \( b^2 = a^n \) as a base case for an inductive proof that \( (a^ib)^2 = a^n \) for \( i = 0, \ldots, 2n-1 \):

\[
(a^ib)^2 = a^iba^ib = a^{i-1}(ab)aa^{i-1}b = a^{i-1}ba^{-1}aa^{i-1}b = a^{i-1}ba^{-1}b = (a^{i-1}b)^2 = a^n \text{ by the inductive hypothesis.}
\]

Now we show that \( (a^ib)^{-1} = a^{n+i}b \) for \( i = 0, \ldots, n-1 \):

\[
(a^ib)(a^{n+i}b) = a^iba^{n-i} = a^{i}a^{n}a^{-n-i} = e
\]

and

\[
(a^{n+i}b)(a^ib) = a^{n+i}bba^{-i} = a^{n+i}a^{n}a^{-i} = a^{2n} = e.
\]

Now for \( i = 0, \ldots, n-1 \), we have \( \langle a^ib \rangle = \{e, a^ib, a^n, a^{n+i}b \} = \langle a^{n+i}b \rangle \). This is a cyclic group of order 4 and so we have \( n \) copies of \( K_4 \) all sharing only the elements \( e \) and \( a^n \) (that is, sharing a copy of \( A \)), and one copy of \( g(\mathbb{Z}_{2n}) \) also containing this copy of \( A \), giving us that \( g(Q_{4n}) \cong g(\langle a \rangle) \cup n(A + K_2) \).

2.4 Abelian groups

We want to work towards describing power graphs of all abelian groups. The Fundamental Theorem of Finite Abelian Groups tells us that abelian groups can be written as products of cyclic groups.

Theorem 2.4 (Fundamental Theorem of Finite Abelian Groups). Every finite abelian group \( G \) can be written as \( G \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}} \) where the \( p_i \) are primes (not necessarily distinct) and the \( m_i \) are positive integers [11, Theorem 11.1].

The proof is omitted in the interest of saving space. A proof can be found in [11, Theorem 11.1].

We start with groups whose non-identity elements have order 2. By Mods Group Theory, these are exactly the groups of the form \( \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \).

Theorem 2.5. For a group \( G \) of finite order \( n \), the following are equivalent:

(i) every non-identity element of \( G \) is of order 2
(ii) \( g(G) \) is a tree
(iii) \( g(G) \cong K_{1,n-1} \)

\[ \Box \text{Theorem 4}. \]

**Lemma 2.1.** For a finite group \( G \) with at least one element of order greater than 2, \( g(G) \) contains a triangle (that is, a copy of \( K_3 \)).

**Proof.** Suppose there is an element \( a \in G \) with \( \text{ord}(a) > 2 \). Then \( e \neq a^2 \neq a \). Since \( G \) is finite, both \( a \) and \( a^2 \) are adjacent to \( e \) in \( g(G) \). Obviously, \( a \) and \( a^2 \) are also adjacent in \( g(G) \), so \( g(G) \) contains a triangle. \( \Box \)

**Proof of Theorem 2.2** (i) \( \implies \) (iii): If every non-identity element of \( G \) has order 2 then obviously \( g(G) \cong K_{1,n-1} \).

(iii) \( \implies \) (ii): Obviously, \( K_{1,n-1} \) is a tree.

(ii) \( \implies \) (i): Assume that at least one element of \( G \) has order greater than 2. Then by Lemma 2.1, \( g(G) \) contains a triangle, and so \( g(G) \) is not a tree. \( \Box \)

Now we describe all power graphs of groups which are products of cyclic groups of the same prime order.

**Theorem 2.6.** For any prime \( p \) and natural number \( n \), \( g((\mathbb{Z}_p)^n) \cong K_1 + \left( \frac{p^n-1}{p-1} \right) K_{p-1} \) \[ 8, \text{Theorem 8} \].

**Proof.** All non-identity elements of \( (\mathbb{Z}_p)^n \) have order \( p \), and so generate a cyclic subgroup of order \( p \) in \( (\mathbb{Z}_p)^n \). Each of these subgroups has \( p - 1 \) generators, and induces a copy of \( K_p \) in \( g((\mathbb{Z}_p)^n) \).

Hence, \( g((\mathbb{Z}_p)^n) \) is made up of copies of \( K_p \) all intersecting only at the identity. We can see this as copies of \( K_{p-1} \) with an extra element linked to every graph vertex. There are \( p^n - 1 \) elements of order \( p \) in the group, and they are partitioned into sets of size \( \phi(p) = p - 1 \) all of which generate the same cyclic subgroup of \( (\mathbb{Z}_p)^n \). Therefore, there are \( \frac{p^n-1}{p-1} \) copies of \( K_{p-1} \), which means \( g((\mathbb{Z}_p)^n) \cong K_1 + \left( \frac{p^n-1}{p-1} \right) K_{p-1} \). \( \Box \)

We generalise the result to groups which are products of cyclic groups of the same prime power order.

**Theorem 2.7.** For any prime \( p \) and two natural numbers \( m \) and \( n \),

\[ g((\mathbb{Z}_{p^m})^n) \cong K_1 + \frac{p^n-1}{p-1} \left( K_{\phi(p^m)} + p^{n-1} \left( K_{\phi(p^2)} + p^{n-1} \left( \cdots + p^{n-1} K_{\phi(p^m)} \cdots \right) \right) \right). \]

**Lemma 2.2.** \( (\mathbb{Z}_{p^m})^n \) has 1 element of order 1, \( p^{(i-1)n}(p^n - 1) \) elements of order \( p^i \) for \( i = 1, \ldots, m \), and no elements of any other order.

**Proof.** The orders of elements of \( (\mathbb{Z}_{p^m})^n \) all divide \( p^m \). There is exactly one element of order 1, the identity.

For \( i = 1, \ldots, m \), the elements of \( (\mathbb{Z}_{p^m})^n \) of order \( p^i \) are exactly the elements which are in the subgroup \( (\mathbb{Z}_{p^i})^n \) of \( (\mathbb{Z}_{p^m})^n \) but not in \( (\mathbb{Z}_{p^{i-1}})^n \), so the number of elements of order \( p^i \) in \( (\mathbb{Z}_{p^m})^n \) is \( |(\mathbb{Z}_{p^i})^n| - |(\mathbb{Z}_{p^{i-1}})^n| = p^m - p^{(i-1)n} = p^{(i-1)n}(p^n - 1) \). \( \Box \)

**Proof of Theorem 2.7.** We show the result by induction on \( m \). The base case where \( m = 1 \) is shown in Theorem 2.4. Now assume that the result is true for \( m \). Because \( (\mathbb{Z}_{p^m})^n \leq (\mathbb{Z}_{p^{m+1}})^n \), we have that \( g((\mathbb{Z}_{p^m})^n) \) is an induced subgraph of \( g((\mathbb{Z}_{p^{m+1}})^n) \), so to construct \( g((\mathbb{Z}_{p^{m+1}})^n) \), we need to draw \( g((\mathbb{Z}_{p^m})^n) \) and then add the vertices which are in \( (\mathbb{Z}_{p^{m+1}})^n \) but not \( (\mathbb{Z}_{p^m})^n \). These are exactly the elements of \( (\mathbb{Z}_{p^{m+1}})^n \) of order \( p^{m+1} \), and since no element generates an element of higher order, the only edges we need to add are the out-edges from the elements of order \( p^{m+1} \) which we added.
By Lemma 2.2 there are \( p^m(p^n - 1) \) elements of order \( p^{n+1} \) in \((\mathbb{Z}_{p^n})^n\), and they can be partitioned into sets of \( \phi(p^{n+1}) \) elements which generate the same cyclic subgroup of \((\mathbb{Z}_{p^n})^n\). So there are \( \frac{p^m(p^n - 1)}{\phi(p^{n+1})} \) cyclic subgroups of order \( p^{n+1} \) in \((\mathbb{Z}_{p^n})^n\). Similarly, there are \( \frac{p^m(p^n - 1)}{\phi(p^{n+1})} \) cyclic subgroups of order \( p^m \). By symmetry, each cyclic subgroup of order \( p^m \) in \((\mathbb{Z}_{p^n})^n\) is contained within the same number of cyclic groups of order \( p^{n+1} \). So every cyclic subgroup of order \( p^n \) in \((\mathbb{Z}_{p^n})^n\) is in

\[
\frac{p^m(p^n - 1)}{\phi(p^{n+1})} \geq \frac{p^m(p^n - 1)\phi(p^m)}{\phi(p^{n+1})} = \frac{p^m(p^{m-1}p - 1)}{p^{m+1}p - 1} = p^{n-1}
\]
different cyclic subgroups of order \( p^{n+1} \).

It is obvious that if \( x, y \in \mathbb{Z}_{p^n+1} \) and \( \langle x \rangle = \langle y \rangle \) then \( x \) and \( y \) are adjacent in \( \mathcal{g}(\mathbb{Z}_{p^n+1}) \), so the generators of each cyclic subgroup of order \( p^{n+1} \) in \( \mathbb{Z}_{p^n+1} \) correspond to a copy of \( K_{\phi(p^{n+1})} \) in \( \mathcal{g}(\mathbb{Z}_{p^n+1}) \). By the induction hypothesis, we have that

\[
\mathcal{g}(\mathbb{Z}_{p^n+1}) \cong K_1 + \frac{p^n - 1}{p - 1} \left( K_{\phi(p^n)} + p^{n-1} \left( \cdots + p^{n-1}K_{\phi(p^n)} \cdots \right) \right),
\]

and each of the copies of \( K_{\phi(p^n)} \) corresponds to one cyclic group of order \( p^n \). Now in \( \mathcal{g}(\mathbb{Z}_{p^n+1}) \) there are \( p^{n-1} \) copies \( K_{\phi(p^{n+1})} \) joined to each one of these copies of \( K_{\phi(p^n)} \) (and the elements of smaller order in the cyclic subgroup of order \( p^n \) which they represent), so we have

\[
\mathcal{g}(\mathbb{Z}_{p^n+1}) \cong K_1 + \frac{p^n - 1}{p - 1} \left( K_{\phi(p^n)} + p^{n-1} \left( \cdots + p^{n-1}K_{\phi(p^{n+1})} \cdots \right) \right).
\]

We have moved some way towards describing power graphs of finite groups which are products of any cyclic groups, which, by the Fundamental Theorem of Finite Abelian Groups (Theorem 2.4), would mean describing the power graphs of all finite abelian groups. It should be possible to find a description of these power graphs, and this could be helpful in showing, as we do in a different way later in this essay, that power graphs of finite abelian groups determine the group up to isomorphism. However, due to time and space constraints, we will not discuss the idea any further in this essay.

## 3 Graph theoretic properties of power graphs

Now that we have specified some power graphs of well-known groups, we discuss some of the properties of power graphs.

### 3.1 Connectivity

It is easy to see that, for a finite group \( G \), \( \mathcal{g}(G) \) is connected [3, Corollary 2.6], since the identity element \( e \in G \) is a power of every other element in \( G \).

In response to a point made at my presentation by Dr Mason Porter, we look at the connectivity of directed power graphs by considering their strongly connected components.

**Definition 3.1.** A directed graph is strongly connected if there is a directed path between each pair of vertices in the graph.

The strongly connected components of a directed graph are the maximal strongly connected subgraphs.

There is no finite group \( G \) for which \( \mathcal{g}(G) \) is strongly connected since there are no out-edges from the identity element in \( \mathcal{g}(G) \). However, we can find the strongly connected components of the directed power graph of any finite group, and hence get a result describing the finite groups that have strongly connected restricted directed power graphs.
Theorem 3.1. For a finite group $G$, the strongly connected components of $\overrightarrow{g}(G)$ are precisely the subgraphs corresponding to the sets of generators of each cyclic subgroup of $G$.

Proof. We first show that, for two distinct group elements $x, y \in G$, there is a path from $x$ to $y$ and a path from $y$ to $x$ if and only if $\langle x \rangle = \langle y \rangle$: if $\langle x \rangle = \langle y \rangle$ then there is a bi-directional edge between $x$ and $y$ in $\overrightarrow{g}(G)$. Conversely, if there is a path $x a_1 a_2 \cdots a_{k-1} y$ from $x$ to $y$ in $\overrightarrow{g}(G)$ then, by definition, $\langle y \rangle \leq \langle a_{k-1} \rangle \leq \cdots \leq \langle a_1 \rangle \leq \langle x \rangle$. Similarly, if there is a path from $y$ to $x$ in $\overrightarrow{g}(G)$ then $\langle x \rangle \leq \langle y \rangle$. So if both paths exist, $\langle x \rangle = \langle y \rangle$.

Now we can see that, for all $g \in G$, the strongly connected component of $\overrightarrow{g}(G)$ which contains $g$ is $\{ x \in G \mid \langle x \rangle = \langle g \rangle \}$. $\square$

Corollary 3.1. For a finite group $G$, $\overrightarrow{g}(G)$ is strongly connected if and only if $G$ is a cyclic group of prime order.

Proof. If $G$ is a cyclic group of prime order, then for every non-identity element $g \in G$, $\langle g \rangle = G$, and so, by Theorem 3.1, $G \setminus \{ e \}$ is a strongly connected component of $\overrightarrow{g}(G)$. This set induces $\overrightarrow{g}(G)$, so $\overrightarrow{g}(G)$ is strongly connected.

Conversely, if $\overrightarrow{g}(G)$ is strongly connected then, by Theorem 3.1, the non-identity elements of $G$ each generate the same cyclic subgroup of $G$. So for all $g \in G \setminus \{ e \}$, the non-identity elements of $G$ are contained in $\langle g \rangle$. The identity is also contained in $\langle g \rangle$, so $\langle g \rangle = G$. This is true for every non-identity element $g$, so $G$ is a cyclic group of prime order. $\square$

Now we look at finite groups that have power graphs with more than one vertex adjacent to every other graph vertex.

Theorem 3.2. Let $G$ be a finite group of order $n = p_1^{m_1} \cdots p_k^{m_k}$ for distinct primes $p_i$, positive integers $m_i$, and $k \geq 1$.

Let $S$ be the set of vertices of $\overrightarrow{g}(G)$ which are adjacent to all other vertices in the graph. Then one of the following cases must hold:

(i) $|S| = 1$,
(ii) $G$ is a generalised quaternion group and $|S| = 2$,
(iii) $G$ is a cyclic group whose order is not a prime power and $|S| = \phi(n) + 1$,
(iv) $G$ is a cyclic group of prime power order and $S = G$.


First, we define a $p$-group as a group where the order of every element is some power of the prime $p$.


There is no room here to prove this lemma, but the reader is encouraged to see Conrad’s proof [9] Theorem 4.7.

Theorem 3.3 (Cauchy’s Theorem). Let $G$ be a finite group. For every prime $p$ dividing $|G|$, there is an element $x \in G$ with order $p$.

This was proved in the group theory course B2b.

Proof of Theorem 3.3 following the proof in [3]. Since $G$ is a finite group, the identity element $e \in G$ is adjacent to all other vertices in $\overrightarrow{g}(G)$, so $|S| \geq 1$.

Suppose $|S| > 1$. Then there is a non-identity group element $g \in S$. For $i = 1, \ldots, k$, by Cauchy’s Theorem (Theorem 3.3), there is an element $x_i \in G$ of order $p_i$. If there is some $j$ such that $p_j \nmid \text{ord}(g)$ then it is easy to see that $x_j \notin \langle g \rangle$ and $g \notin \langle x_j \rangle$, and so $g \notin S$, which is a contradiction. So every prime divisor of $|G|$ also divides the order of $g$. 

10
We now take two cases for $|G|$. First, suppose $k = 1$, which means $G$ is a $p$-group for some prime $p$. Then $p \nmid \text{ord}(g)$, so by Cauchy’s Theorem (Theorem 3.3), there is an element $x \in \langle g \rangle$ such that $\text{ord}(x) = p$. We show that $\langle x \rangle$ is the only subgroup of $G$ of order $p$: if $y \in G \setminus \langle g \rangle$ is also of order $p$ then, since $\text{ord}(y) \leq \text{ord}(g)$, $y$ is not adjacent to $g$, contradicting the fact that $g \in S$.

Now by Lemma 3.1 since $G$ is a finite $p$-group with a unique subgroup of order $p$, it must be cyclic or generalised quaternion. If $G$ is generalised quaternion then from Proposition 2.2 we can see that $S = \{c, c^n\}$, so $|S| = 2$. If $G$ is cyclic then by Theorem 2.1 $S = G$.

The second case is that $k = 2$ and so $|G|$ is divisible by at least two distinct primes. By Cauchy’s Theorem (Theorem 3.3), if $p$ is a prime dividing $|G|$ then there is an element $x$ of order $p$ in $G$. Since $\text{ord}(x) \leq \text{ord}(g)$, if $x \notin \langle g \rangle$ then $x$ is not adjacent to $g$ in $g(G)$, which contradicts the fact that $g \in S$. Therefore, $\langle g \rangle$ contains every subgroup of $G$ of prime order, and since $\langle g \rangle$ is cyclic, $G$ contains exactly one subgroup of order $p$ for each prime $p$ dividing $|G|$. So $G$ is cyclic.

Since $G$ is cyclic and not of prime power order, it follows that, for all $x \in S$, $\langle x \rangle = G$. It is also easy to see that if $\langle x \rangle = G$ then $x \in S$. So $|S| = \phi(n) + 1$.

There are no other cases for $G$, so we are done.

3.2 Total valency

Definition 3.2. For an undirected graph $H$, the degree $d_H(x)$ of a graph vertex $x$ is the number of vertices adjacent to $x$ in $H$. When $H$ is a digraph, we can define $d_H^+(x)$ and $d_H^-(x)$ to be respectively the in-degree (number of vertices that have an edge to $x$ in $H$) and out-degree (number of vertices that have an edge from $x$ in $H$) of $x$ in $H$.

For a group $G$, define the total valency $D(G)$ of $G$ to be the sum of the degrees of the vertices in the power graph of $G$

\[ D(G) = \sum_{g \in G} d_{\phi(G)}(g), \]

and the total in-valency and total out-valency of $G$ to be the sums of in- and out-degrees of vertices in the directed power graph of $G$ respectively:

\[ D^-(G) = \sum_{g \in G} d^-_{\phi(G)}(g), \quad D^+(G) = \sum_{g \in G} d^+_{\phi(G)}(g). \]

Notation 3.1. When it is obvious which group we are talking about, we write $d(g)$, $d^-(g)$, and $d^+(g)$.

Proposition 3.1. For a finite group $G$ of order $n$ and an element $g \in G$,

(i) $d^+(g) = \text{ord}(g) - 1$.

(ii) The number of bi-directional edges incident on $g$ in $g(G)$ is $\phi(\text{ord}(g)) - 1$.

(iii) $d(g) = \text{ord}(g) - \phi(\text{ord}(g)) + d^-(g)$.

(iv) $d^-(e) = n - 1$ and $d^+(e) = 0$.

(v) $d^-(g)$ is odd if $\text{ord}(g) \geq 3$ and even if $\text{ord}(g) = 2$.

(vi) Suppose $g$ is not the identity. If $\text{ord}(g)$ is odd then $d(g)$ is even, and if $\text{ord}(g)$ is even then $d(g)$ is odd.

Proof. (i) Obviously, $d^+(g) = |\langle g \rangle \setminus \{g\}| = \text{ord}(g) - 1$.

(ii) The group elements which share a bi-directional edge with $g$ in $g(G)$ are precisely the elements $x \in \langle g \rangle$ such that $\langle x \rangle = \langle g \rangle$ and $x \neq g$. So the number of bi-directional edges incident on $g$ is $|\{x \in \langle g \rangle | \langle x \rangle = \langle g \rangle\} \setminus \{g\}| = \phi(\text{ord}(g)) - 1$.

(iii) To calculate $d(g)$, we count the number of out-edges from $g$ and in-edges to $g$, and then take the number of bi-directional edges incident on $g$. So by (i) and (ii), $d(g) = d^+(g) + d^-(g) - (\phi(\text{ord}(g)) - 1) = \text{ord}(g) - \phi(\text{ord}(g)) + d^-(g)$.
(iv) Obviously, $e \in \langle a \rangle$ for all $a \in G$, and $\langle e \rangle = \{e\}$.
(v) $d^-(g) = |\{a \in G \mid g \in \langle a \rangle\}|$ and if $g \in \langle a \rangle$ then $g \in \langle a^{-1} \rangle = \langle a \rangle$. Obviously, $g \in \langle g \rangle$.
So $|\{a \in G \mid g \in \langle a \rangle\}| = \{a, a^{-1} \mid g \in \langle a \rangle \} \setminus \{g\}$. So $d^-(g) = |\{a, a^{-1} \mid g \in \langle a \rangle \} \setminus \{g\}|$ is odd for $\text{ord}(g) \geq 3$, since $g \neq g^{-1}$. Similarly, $d^+(g) = |\{a, a^{-1} \mid g \in \langle a \rangle \} \setminus \{g\}|$ is even for $\text{ord}(g) = 2$, since $g = g^{-1}$.
(vi) By (iii), we have $d(g) = \text{ord}(g) - \phi(\text{ord}(g)) + d^-(g)$. For $\text{ord}(g) = 2$, we have $\phi(\text{ord}(g)) = 1$ and $d^-(g)$ is even by (v), so $d(g) = \text{ord}(g) - \phi(\text{ord}(g)) + d^-(g) = 1 + d^-(g)$ which is odd. If $\text{ord}(g) \geq 3$, then $\phi(\text{ord}(g))$ is even and, by (v), $d^-(g)$ is odd. So $d(g) = \text{ord}(g) - \phi(\text{ord}(g)) + d^+(g)$ is odd if $\text{ord}(g)$ is even, and even if $\text{ord}(g)$ is odd.

**Proposition 3.2.** For a finite group $G$, $D^+(G) = D^-(G) = \left(\sum_{g \in G} \text{ord}(g)\right) - |G|$.

**Proof.** Since $d^+(g) = \text{ord}(g) - 1$,

$$D^+(G) = \sum_{g \in G} d^+(g) = \sum_{g \in G} \text{ord}(g) - 1 = \left(\sum_{g \in G} \text{ord}(g)\right) - |G|.$$ 

$D^-(G) = D^+(G)$ because each edge has two endpoints, and so there is one in-edge to every out-edge in the graph.

Chakrabarty, Ghosh and Sen give a formula for the total valency of a finite group.

**Theorem 3.4.** For a finite group $G$, the total valency is given by

$$D(G) = \sum_{g \in G} 2\text{ord}(g) - \phi(\text{ord}(g)) - 1$$


**Proof.** We look at $\tilde{g}(G)$. We want to count twice the number of edges. For each vertex, we count bi-directional edges incident on the vertex once, and other out-edges twice, in total counting each edge once for each end-point. If we count every out-edge from $g \in G$ twice, giving us $2(\text{ord}(g) - 1)$, we have overcounted by the number of bi-directional edges incident on $g$, which, by Proposition 3.1(ii), is $\phi(\text{ord}(g)) - 1$. So each vertex $g \in G$ contributes $2(\text{ord}(g) - 1) - (\phi(\text{ord}(g)) - 1) = 2\text{ord}(g) - \phi(\text{ord}(g)) - 1$ to the total valency. Note that this does not give us a formula for $d(g)$, but we have ensured that we count each endpoint of each edge exactly once. Therefore, $D(G) = \sum_{g \in G} 2\text{ord}(g) - \phi(\text{ord}(g)) - 1$ as required.

**Corollary 3.2.** For $G$ a finite cyclic group of order $n$, $D(G) = \sum_{d|n} (2d - \phi(d) - 1)\phi(d)$ [6, Corollary 4.3].

**Proof.** Every element of the group has order $d$ dividing $n$, and there are $\phi(d)$ elements of each order $d \mid n$, so the result follows from Theorem 3.4.

### 3.3 Planarity

**Definition 3.3.** A plane graph is a graph that is drawn in the plane with no two edges intersecting. A planar graph is a graph that is isomorphic to some plane graph.

We require the following result from B11b Graph Theory.

**Theorem 3.5.** $K_5$ is not planar [3, pp. 23].

**Theorem 3.6.** If $\Gamma_1$ is a graph with a non-planar subgraph $\Gamma_2$, then $\Gamma_1$ is not planar.

**Proof.** Obvious.
**Theorem 3.7.** For a finite cyclic group $G$ of order $n$, $g(G)$ is planar if and only if $n < 5$. [4, Theorem 2.2].

**Lemma 3.2.** For an integer $n > 6$ or $n = 5$, $\phi(n) \geq 4$.

**Proof.** Let $n = p_1^{m_1} \cdots p_k^{m_k}$. Then $\phi(n) = p_1^{m_1-1}(p_1 - 1) \cdots p_k^{m_k-1}(p_k - 1)$ by Part A Number Theory. Suppose $\phi(n) < 4$. The only primes that can divide $n$ are 2 and 3. We cannot have $2^3$, $3^2$ or $2^23$ dividing $n$, so we must have $n = 1, 2, 3, 4, 6$.

**Proof of Theorem 3.7.** Suppose $n \geq 5$ and $n \neq 6$. Then, by Lemma 3.2, $\phi(n) \geq 4$. If $n$ is a composite number, then, by Theorem 3.2, there are $\phi(n) + 1 \geq 5$ vertices connected to all other vertices in $g(Z_n)$, and so $g(Z_n)$ contains a copy of $K_5$. If $n$ is a prime power then, by Theorem 2.1, $g(Z_n)$ is complete and so contains a copy of $K_5$. In both cases, $g(Z_n)$ contains a copy of the non-planar graph $K_5$ and so, by Theorem 3.6, $g(Z_n)$ is not planar.

In the case that $n = 6$, the diagram of $g(Z_6)$ in Figure 6 highlights its $K_5$ subgraph, which shows that $g(Z_6)$ is non-planar by Theorem 3.5 and Theorem 3.6.

Conversely, to show that $g(Z_n)$ is planar for $n < 5$, we give plane drawings of $g(Z_n)$ for $n = 1, 2, 3, 4$ in Figure 7. These are all complete by Theorem 2.1.

We can use this to find a necessary and sufficient condition on finite groups for their undirected power graphs to be planar. We resolve, in the affirmative, a conjecture of Mirzargar, Ashrafi, Nadjafi-Arani [15, Corollary to Conjecture 1], which is misquoted as a theorem in the literature review [1, Theorem 11.1].

---

Figure 6: $g(Z_6)$ with the edges of its $K_5$ subgraph in solid black and other edges in dashed blue.

Figure 7: Plane drawings of $g(Z_n)$ for $n = 1, 2, 3, 4$ from left to right.
Theorem 3.8. Let $G$ be a finite group. Then $\mathfrak{g}(G)$ is planar if and only if every element of $G$ is of order 1, 2, 3, or 4 [15, Corollary to Conjecture 1].

Proof. If there is an element $a \in G$ of order $\text{ord}(a) = m > 4$, then $\langle a \rangle \cong \mathbb{Z}_m$, and so by Theorem [3.7] $\mathfrak{g}(\langle a \rangle)$ is non-planar. Now $\langle a \rangle \leq G$ and so by Theorem [3.6] $\mathfrak{g}(G)$ is non-planar. So if $\mathfrak{g}(G)$ is planar then every element is of order 1, 2, 3, or 4.

Conversely, suppose the elements of $G$ are all of order 1, 2, 3, or 4. Every element $g$ of order 4 is adjacent only to elements in $\langle g \rangle$, since there are no elements of order greater than 4. So the elements of orders 2 and 4 form collections of triangles all of which share one element of order two. So if there are $k$ elements of order 2 in $G$, the elements of orders 2 and 4 induce the graph $\bigcup_{i=1}^{k} (K_1 + a_iK_2)$ in $\mathfrak{g}(G)$ for some non-negative integers $a_i$ (not necessarily distinct). Note that there are $2(a_1 + \cdots + a_k)$ elements of order 4 in $G$.

The elements of order 3 are adjacent only to their inverse and the identity, so if there are $t$ elements of order 3, they induce a collection of $t$ disjoint line segments $tK_2$ in $\mathfrak{g}(G)$.

No element of order 3 can be adjacent to any element of order 2 or 4. We can see from Figure [8] that it is possible to connect one point to all of the vertices of our triangles and line segments, so connecting the identity to every group element and completing a plane drawing of the graph $\mathfrak{g}(G) \cong \left( \bigcup_{i=1}^{k} (K_1 + a_iK_2) \cup \frac{t}{2}K_2 \right) + K_1$.

So if every element of $G$ is of order 1, 2, 3, or 4, then $\mathfrak{g}(G)$ is planar. 

Note that, in our proof of this result, we have also shown that every non-planar power graph of a finite group contains a copy of $K_5$.

3.4 Euler circuits and trails

Definition 3.4. An Euler circuit in a graph $\Gamma$ is a closed walk containing all edges of $\Gamma$ exactly once.

An Euler trail in a graph $\Gamma$ is a walk which is not closed and contains all edges of $\Gamma$ exactly once.
Lemma 3.3. A connected graph $\Gamma$ has an Euler circuit if and only if the degree of every graph vertex is even $[3]$ Theorem 12).

Proof. The result is proved in the B11b Graph Theory course.

Corollary 3.3. A connected graph $\Gamma$ has an Euler trail if and only if there are exactly two distinct vertices in $\Gamma$ of odd degree $[3]$ pp. 17].

Proof, following the proof in $[3]$. If $u$ and $v \neq u$ are the only vertices of odd degree in $\Gamma$, then we define $\Gamma'$ to be $\Gamma$ with an extra vertex $x$ and two extra edges $ux$ and $xv$. It is obvious that every vertex of $\Gamma'$ has even degree, and so, by Lemma 3.3, there is an Euler circuit $C'$ in $\Gamma'$. We set $C = C' - x$, the Euler circuit in $\Gamma'$ without the edges $ux$ or $xv$. It is easy to see that this is an Euler trail in $\Gamma$.

Conversely, if $\Gamma$ has an Euler trail then it must have two endpoints $u$ and $v \neq u$. The trail must go through $u$ and $v$ an odd number of times to avoid closing the walk, and must go through the other graph vertices an even number of times in order to include all graph edges. Since the trail contains all of the graph edges, $u$ and $v$ must have odd degrees and the other vertices in the graph must have even degrees.

Theorem 3.9. For a finite group $G$ of order $n$, $g(G)$ has an Euler circuit if and only if $n$ is odd $[5]$ Theorem 6].

Proof. If $n$ is even then $d(e) = n - 1$ which is odd, and so $g(G)$ does not have an Euler circuit by Lemma 3.3.

Conversely, we suppose that $n$ is odd. Then $d(e) = n - 1$ which is even. For all non-identity elements $a \in G$, $\text{ord}(a) | n$, so $\text{ord}(a)$ must be odd. Then by Proposition 3.1(vi), $d(a)$ is even. The degree of every vertex is even, so, by Lemma 3.3, $g(G)$ has an Euler circuit.

Theorem 3.10. For a finite group $G$, $g(G)$ has an Euler trail if and only if $G$ has exactly one element of even order.

Proof. Suppose $g(G)$ has an Euler trail. If $|G|$ is odd then by Theorem 3.9, $G$ has an Euler circuit, and therefore no Euler trail. So $|G|$ must be even, meaning $d(e) = n - 1$ is odd. Therefore by Corollary 3.3 there is exactly one non-identity element $g \in G$ with odd degree in $g(G)$. By Proposition 3.1, $d(g)$ is odd if and only if $\text{ord}(g)$ is even. So there is exactly one element of even order in $G$.

Conversely, suppose $G$ has exactly one element $g$ of even order. Then by Proposition 3.1, $d(g)$ is odd. Since $G$ has an element of even order, $|G|$ is even, and so $d(e) = n - 1$ is odd. For all $a \in G \setminus \{e, g\}$, we know $\text{ord}(a)$ is odd and so by Proposition 3.1, $d(g)$ is even. So $g(G)$ has exactly two distinct vertices $e$ and $g$ of odd degree, and by Corollary 3.3, $g(G)$ has an Euler trail.

Corollary 3.4. For a finite group $G$, $g(G)$ has an Euler trail if and only if $G$ is the cyclic group of order 2.

Proof. Let $G$ be a finite group. By Theorem 3.10 if $g(G)$ has an Euler trail then $G$ has exactly one element $x \in G$ of even order. By Cauchy’s Theorem [Theorem 3.3], since the prime 2 divides $|\langle x \rangle|$, there must be an element of order 2 in $\langle x \rangle$. Since $x$ is the only element of $G$ of even order, we conclude $\text{ord}(x) = 2$. Now let $y \in G$ be an element of odd order. We know $\text{ord}(gy^{-1}) = \text{ord}(x) = 2$, and there is only one element of even order, so we must have $yxy^{-1} = x$. Therefore, $x$ and $y$ commute, so $x$ has even order. Again, since $x$ is the only element of even order, $xy = x$. So $y$ is the identity element, and $G$ is the cyclic group of order 2.

The converse is obvious.
4 The automorphism group of a power graph

Definition 4.1. An automorphism of a finite group $G$ is a permutation $\pi : G \to G$ which preserves the group operation, that is, $\pi(ab) = \pi(a)\pi(b)$ for all $a, b \in G$. The automorphisms of a group $G$ form a group $\text{Aut}(G)$ under composition.

An automorphism of a graph $\Gamma = (V, E)$ is a permutation $\sigma : V \to V$ which preserves edge relations, that is, $(u, v) \in E$ if and only if $(\sigma(u), \sigma(v)) \in E$. The automorphisms of a graph $\Gamma$ form a group $\text{Aut}(\Gamma)$ under composition.

It is obvious that for a finite group $G$, a group automorphism induces an automorphism of the graph $g(G)$, and that no two group automorphisms induce the same graph automorphism. This means that $\text{Aut}(G) \leq \text{Aut}(g(G))$. In fact, there is only one non-trivial finite group which has the same automorphism group as its power graph.

Theorem 4.1. For a finite group $G$, $\text{Aut}(G) = \text{Aut}(g(G))$ if and only if $G$ is the Klein four group $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $G$ is trivial [5] Theorem 5].

First we need the following lemma:

Lemma 4.1. $\text{Aut}((\mathbb{Z}_2)^n) = \text{GL}(n, 2)$ and $|\text{Aut}((\mathbb{Z}_2)^n)| = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1})$.

Proof. We can view $(\mathbb{Z}_2)^n$ as an $n$-dimensional vector space of the field with two elements. We know from Part A Linear Algebra that the vector space automorphisms are the invertible linear transformations from the vector space to itself, so $\text{Aut}((\mathbb{Z}_2)^n) = \text{GL}(n, 2)$. Part A Linear Algebra also gives us that $|\text{GL}(n, 2)| = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1})$. □

Proof of Theorem 4.1 following the proof in [5]. Let $G$ be a finite group such that $\text{Aut}(G) = \text{Aut}(g(G))$.

The map $\pi$ defined for all $g \in G$ by $\pi : g \mapsto g^{-1}$ is in $\text{Aut}(g(G))$ since $\langle g \rangle = \langle g^{-1} \rangle$. If $\pi \in \text{Aut}(G)$ then, for all $a, b \in G$, we have $b^{-1}a^{-1} = (ab)^{-1} = \pi(ab) = \pi(a)\pi(b) = a^{-1}b^{-1}$, and so we get $ab = ba$. Hence, $G$ must be abelian.

In an abelian group $G$, if there is an element $a$ of order greater than 2 and a group element $g \notin \langle a \rangle$ whose order divides $\text{ord}(a)$, then the element $ag$ of order $\text{ord}(a) > 2$ is not equal to $a$, $g$ or $(ag)^{-1}$. There is an automorphism $\pi \in \text{Aut}(g(G))$ which sends $ag$ to $(ag)^{-1}$ and fixes $a$ and $g$. But if $\pi$ is an automorphism of $G$ then $ag = \pi(a)\pi(g) = \pi(ag) = (ag)^{-1}$, which is a contradiction. So $\pi \notin \text{Aut}(G)$.

It follows that there cannot be an element $a$ of order greater than 2 and an element $g \notin \langle a \rangle$ whose order divides that of $a$. So if there is an element in $G$ of order greater than 2 then for any such element $a$, for all $g \in G$ whose order divides $\text{ord}(a)$, $g \in \langle a \rangle$, and so $G$ is cyclic. Otherwise, all non-identity elements of $G$ have order 2, so $G \cong (\mathbb{Z}_2)^n$ for some positive integer $n$.

If $G$ is cyclic and non-trivial, then $G \cong \langle g \rangle$ where $g$ is some non-identity element of $G$. The identity and the generators of the group are connected to all other elements, so $g$ and $e$ are connected to the same elements as each other. Therefore, there is an automorphism $\pi$ of the power graph of $G$ which swaps $g$ and $e$, and fixes the rest of the group, but $\pi \notin \text{Aut}(G)$ since group automorphisms must fix the identity.

If $G$ is the trivial group then $\text{Aut}(g(G)) = \{e\} = \text{Aut}(G)$.

If $G \cong (\mathbb{Z}_2)^n$ then, by Theorem 2.5, $g(G) \cong K_{1,2^n-1}$ and $\text{Aut}(g(G)) \cong \text{Sym}(2^n - 1)$. By Lemma 4.1, $\text{Aut}((\mathbb{Z}_2)^n) = \text{GL}(n, 2)$. For $n = 2$, we get $|\text{Aut}(g((\mathbb{Z}_2)^n))| = |\text{Sym}(2^2 - 1)| = (2^2 - 1)! = 2^2 - 1! = (2^2 - 1)(2^2 - 2) = |\text{GL}(n, 2)| = |\text{Aut}((\mathbb{Z}_2)^n)| = 6$. However, for $n > 2$, $|\text{Sym}(2^n - 1)| = (2^n - 1)! > (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}) = |\text{GL}(n, 2)|$. So since $\text{Aut}((\mathbb{Z}_2)^n) \leq \text{Aut}(g((\mathbb{Z}_2)^n))$, we have that $\text{Aut}(g((\mathbb{Z}_2)^n)) = \text{Aut}((\mathbb{Z}_2)^n)$ if and only if $n = 2$. Now we have the result that $\text{Aut}(G) = \text{Aut}(g(G))$ if and only if $G$ is trivial or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □
This naturally leads us to ask which finite groups have the same automorphism group as their directed power graph.

**Theorem 4.2.** For a finite group $G$, $\text{Aut}(G) = \text{Aut}(\vec{g}(G))$ if and only if $G$ is the Klein four group $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_n$ for $n = 1, 2, 3, 4$.

We will find the following lemma useful in our proof:

**Lemma 4.2.** If $G$ is a cyclic group of order $n$ then $\text{Aut}(G) \cong (\mathbb{Z}_n)^*$, the group of generators of the cyclic group of order $n$.

**Proof.** For some $x \in G$, $G = \langle x \rangle$. So we can write every element as a power of $x$. If $\pi \in \text{Aut}(G)$ then $\pi(x^k) = \pi(x)^k$ and so $\pi$ is completely specified by what it does to $x$. With an automorphism, we can move $x$ to any generator of $G$, and to no other elements, so there is one automorphism for each generator of $G$. Since $x$ was arbitrary, we have $\text{Aut}(G) \cong (\mathbb{Z}_n)^*$.

**Proof of Theorem 4.2.** In our proof of Theorem 4.1, we showed that if the automorphism group of $G$ is the same as the automorphism group of the undirected power graph of $G$ then $G$ must be $(\mathbb{Z}_2)^n$ or cyclic. The same argument holds if we replace the undirected power graph with the directed power graph.

If $\text{Aut}(G) = \text{Aut}(\vec{g}(G))$ then $G$ must be $(\mathbb{Z}_2)^n$ or cyclic.

If $G$ is cyclic with $|G| = 5$ or $|G| > 6$, then by Lemma 3.2, there are at least four distinct generators $x, x^{-1}, y, y^{-1}$ of $G$. If $|G| = 6$ then there are only two distinct generators of the group, however, in this case, we can let $x, x^{-1}$ be the elements of $G$ of order 6 and $y = x^2, y^{-1} = x^4$ be the elements of order 3. In both cases, there is an automorphism $\pi \in \text{Aut}(\vec{g}(G))$ which fixes $x$ and $x^{-1}$ and swaps $y$ and $y^{-1}$. Since $y \in \langle x \rangle$, we have $y = x^k$ for some positive integer $k$ (in the case that $|G| = 6, k = 2$). Now if $\pi \in \text{Aut}(G)$, we get $y^{-1} = \pi(y) = \pi(x^k) = \pi(x)^k = x^k = y$ which is a contradiction since $\text{ord}(y) > 2$. So we can see that $\pi \notin \text{Aut}(G)$.

So if $G$ is a cyclic group then it must have order 1, 2, 3 or 4. We know by Lemma 4.2 that $\text{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n)^*$. In Figure 9, we can see that

$$
\text{Aut}(\vec{g}(\mathbb{Z}_1)) \cong \{e\} \cong (\mathbb{Z}_1)^* \cong \text{Aut}(\mathbb{Z}_1),
\text{Aut}(\vec{g}(\mathbb{Z}_2)) \cong \{e\} \cong (\mathbb{Z}_2)^* \cong \text{Aut}(\mathbb{Z}_2),
\text{Aut}(\vec{g}(\mathbb{Z}_3)) \cong \text{Sym}(2) \cong (\mathbb{Z}_3)^* \cong \text{Aut}(\mathbb{Z}_3), \text{ and }
\text{Aut}(\vec{g}(\mathbb{Z}_4)) \cong \text{Sym}(2) \cong (\mathbb{Z}_4)^* \cong \text{Aut}(\mathbb{Z}_4),
$$

so $\text{Aut}(\vec{g}(\mathbb{Z}_n)) \cong \text{Aut}(\mathbb{Z}_n)$ if and only if $n = 1, 2, 3, \text{ or } 4$.

If $G \cong (\mathbb{Z}_2)^n$ then $\vec{g}(G)$ is a star graph which has $2^n - 1$ elements all with an out-edge to the identity element, and no other edges. Then $\text{Aut}(\vec{g}(G)) = \text{Sym}(2^n - 1) = \text{Aut}(\vec{g}(G))$ so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by Theorem 4.1.

So if $\text{Aut}(G) = \text{Aut}(\vec{g}(G))$ then $G$ can only be cyclic of order less than 5 or the Klein four group.
5 How much information about a group does its power graph carry?

It is natural to ask how much we know about a group given its power graph.

In general, the power graph does not determine the group. For example, as Cameron and Ghosh [5] point out, if $G$ is a finite group of order $n$ in which every non-identity element is of order 3 then $g(G) \cong K_1 + \frac{n-1}{2}K_2$. So $g(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3) \cong K_1 + 13K_2$. There is also a non-abelian group $H = \langle x, y \mid x^3 = y^3 = (x^{-1}y^{-1}xy)^3 = e \rangle$ of order 27 whose non-identity elements are all of order 3, so $g(H) \cong g(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)$ but the groups are not isomorphic since $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ is abelian.

In fact, the same example works to show that the directed power graph does not determine the group. The graph of $\bar{g}(H) \cong \bar{g}(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)$ is shown in Figure 5.

We can, however, determine the group given its power graph if we know the group is abelian. We show that we can recover the element orders of a finite group from its directed power graph [5], and that this means that, for finite abelian groups, the directed power graph determines the group up to isomorphism [5]. We also show that, for finite groups, the undirected power graph determines the directed power graph up to isomorphism [4].

**Definition 5.1.** Two finite groups $G$ and $H$ are conformal if they have the same number of elements of each order.

**Proposition 5.1.** Let $G$ and $H$ be finite groups such that $\bar{g}(G) \cong \bar{g}(H)$. Then $G$ and $H$ are conformal [5, Proposition 4].

**Proof.** Since the power graphs are directed, we can very easily calculate $d^+(g)$ for all $g \in G$ by counting the out-edges from $g$. Then, by Proposition [3.1] we see that $d^+(g) + 1 = \text{ord}(g)$, and so the graph specifies how many elements of each order are in the group. So if $\bar{g}(G) \cong \bar{g}(H)$ then $G$ and $H$ are conformal. \hfill \qedsymbol
Theorem 5.1. If two finite abelian groups $G$ and $H$ are conformal then they are isomorphic \[5\] pp. 95.

Lemma 5.1. If $G \cong (\mathbb{Z}_p)^{a_1} \times (\mathbb{Z}_p)^{a_2} \times \cdots \times (\mathbb{Z}_p)^{a_k}$ for some prime $p$ and non-negative integers $a_i$, then for $i = 1, 2, \ldots, k$, and letting $m_i = a_i + \cdots + a_k$, there are

$$p^{a_1} p^{a_2} \cdots p^{(i-1)a_{i-1}} p^{(i-1)m_i} (p^{m_i} - 1)$$

elements of order $p^i$ in $G$.

Proof. For $x = (x_1, 1, \ldots, x_{a_1}, 1, \ldots, x_{a_1}, 1, \ldots, x_{a_k}, 1, \ldots, x_{a_k}) \in G$, $\text{ord}(x) = \max(\text{ord}(x_1), \ldots, \text{ord}(x_{a_1}))$. Fix $i$. We want to find all elements $x$ of order $p^i$. For $j = 1, \ldots, i - 1$, the co-ordinate $x_{j, l}$ for $l = 1, \ldots, a_i$ can take any of $p^j$ values, since none of these can be of order greater than $p^j$. Then for $r = i, \ldots, k$ and $n = 1, \ldots, a_r$, we need to choose $x_{r, n}$ to be of order $p^i$, with at least one co-ordinate being of order $p^j$. This is the same as picking an element of order $p^i$ from $(\mathbb{Z}_p)^{m_i}$ where $b \geq i$, and by Lemma 2.2, $(\mathbb{Z}_p)^{m_i}$ has $p^{(i-1)m_i} (p^{m_i} - 1)$ elements of order $p^i$ for $i = 1, \ldots, b$.

So there are $p^{a_1} p^{a_2} \cdots p^{(i-1)a_{i-1}}$ choices for the first $i - 1$ co-ordinates of an element of order $p^i$ in $G$ and $p^{(i-1)m_i} (p^{m_i} - 1)$ choices for the remaining co-ordinates, giving us

$$p^{a_1} p^{a_2} \cdots p^{(i-1)a_{i-1}} p^{(i-1)m_i} (p^{m_i} - 1)$$

elements of order $p^i$ in $G$. \(\square\)

Proof of Theorem 5.1. First, we show that if abelian groups $G$ and $H$ have the same number of elements of each prime power order then they must be conformal.

Suppose $G$ is a finite abelian group. Given $n = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$ for distinct primes $q_i$, positive integers $b_i$ and some integer $k$ such that $n$ divides $|G|$, we want to find the number of elements in $G$ of order $n$. Let $y_i$ be the number of elements of order $q_i^{b_i}$ in $G$. Then, since $G$ is abelian, it is obvious that there are $y_1 y_2 \cdots y_k$ elements of order $n$ in $G$.

So given the number of elements of each prime power order in $G$, we know the number of elements of every order in $G$.

So we only need to consider the case where $G$ and $H$ have prime power order.

Suppose $G$ and $H$ are conformal. Then they must have the same total number of elements, so let $|G| = |H| = p^l$ for some prime $p$ and positive integer $l$ (the trivial case is obvious). Let $k$ be the positive integer such that the highest element order in $G$ is $p^k$. Then, since $G$ and $H$ are conformal, $p^k$ is also the highest element order in $H$. By the Fundamental Theorem of Finite Abelian Groups (Theorem 2.4), and the fact that the order of every element of $G$ and $H$ is a power of $p$, we can write $G \cong (\mathbb{Z}_p)^{a_1} \times (\mathbb{Z}_p)^{a_2} \times \cdots \times (\mathbb{Z}_p)^{a_k}$ and $H \cong (\mathbb{Z}_p)^{b_1} \times (\mathbb{Z}_p)^{b_2} \times \cdots \times (\mathbb{Z}_p)^{b_k}$ for some non-negative integers $a_i$ and $b_i$.

Let $m_i = a_i + \cdots + a_k$ and $n_i = b_i + \cdots + b_k$. Then for $i = 1, \ldots, k$, since $G$ and $H$ have the same number of elements of order $p^i$ and by Lemma 5.1 we have

$$p^{a_1} p^{a_2} \cdots p^{(i-1)a_{i-1}} p^{(i-1)m_i} (p^{m_i} - 1) = p^{b_1} p^{b_2} \cdots p^{(i-1)b_{i-1}} p^{(i-1)n_i} (p^{n_i} - 1).$$

To simplify this, let $\alpha_i = a_1 + 2a_2 + \cdots + (i - 1)a_{i-1} + (i - 1)m_i$ and $\beta_i = b_1 + 2b_2 + \cdots + (i - 1)b_{i-1} + (i - 1)n_i$. Then we have $p^{\alpha_i} (p^{m_i} - 1) = p^{\beta_i} (p^{n_i} - 1)$. If $\alpha \neq \beta$, then, without loss of generality, we can assume $\alpha > \beta$, and so $p^{\alpha - \beta} (p^{m_i} - 1) = (p^{n_i} - 1)$, but then since $p | p^{\alpha - \beta} (p^{m_i} - 1)$, we must also have $p | (p^{n_i} - 1)$ giving us a contradiction. So we know that $\alpha = \beta$.

This gives us that $p^{m_i} - 1 = p^{n_i} - 1$, and so we have $m_i = n_i$ for all $i$.

By definition, $a_1 = m_1$ and $a_i = m_i - (a_{i-1} + \cdots + a_1)$. So, with $m_i = n_i$, we have that $a_i = b_i$ for $i = 1, \ldots, k$, and therefore $G \cong H$. \(\square\)

Corollary 5.1. For $G$ and $H$ finite abelian groups, $\overline{\mathfrak{g}}(G) \cong \overline{\mathfrak{g}}(H)$ if and only if $G \cong H$. \[5\]
Definition 5.2. For a group $G$, the closed neighbourhood $N(g)$ of $g \in G$ is the set containing the group elements adjacent to $g$ in the power graph $\tilde{g}(G)$ and the element $g$ itself.

Theorem 5.2. If $G$ and $H$ are finite groups then $\tilde{g}(G) \cong \tilde{g}(H)$ if and only if $\tilde{g}(G) \cong \tilde{g}(H)$ [H, Theorem 2].

We will extend this result to undirected power graphs by showing that the undirected power graph determines the directed power graph up to isomorphism.

Definition 5.3. For a finite group $G$ and elements $x, y \in G$, say $\equiv$ if and only if $N(x) = \bar{N}(y)$ in $\tilde{g}(G)$, and $\approx$ if and only if $\langle x \rangle = \langle y \rangle$.

It is obvious that $\equiv$ and $\approx$ are both equivalence relations. From the above Lemma, we get the following Corollary of Cameron.

Corollary 5.2 (Corollary of Lemma [5.2]). Let $G$ be a finite group and $C$ be a non-identity $\equiv$-class of $g(G)$. Then $C$ can be categorised as one of the following types:

(i) $C$ is a $\approx$-class. In this case, $|C| = \phi(\text{ord}(y))$ for any $y \in C$.

(ii) There is an element $y \in C$ of order $\text{ord}(y) = p^r$ for some prime $p$ and positive integer $r$ such that $C = \{z \in \langle y \rangle | \text{ord}(z) > p^s\}$ for some $s < r - 1$. In this case, $C$ is the union of $r - s \approx$-classes, and so $|C| = p^r - p^s$.

Proof. If $C$ contains an element not of prime power order then it follows directly from Lemma [5.2] that $C$ is a $\approx$-class.

If every element of $C$ has prime power order, then it follows directly from Lemma [5.2] that there is an element $y \in C$ of order $\text{ord}(y) = p^r$ for some prime $p$ and positive integer $r$, and some $s \leq r - 1$, such that $C = \{z \in \langle y \rangle | \text{ord}(z) > p^s\}$. If $s = r - 1$ then every element of $C$ has the same order, and so $C$ is a $\approx$-class.

If $s < r - 1$ then it is obvious that $C = \{z \in \langle y \rangle | \text{ord}(z) > p^s\}$, the union of $r - s \approx$-classes, one made up of elements of order $p^{s+1}$, one made up of elements of order $p^{s+2}$, ..., and one made up of elements of order $p^r$.

For any $g \in G$, the size of the $\approx$-class containing $g$ is $\phi(\text{ord}(g))$, so if $C$ is a $\approx$-class, then $|C| = \phi(\text{ord}(g))$ for any $y \in C$, and if $C$ is a union of $r - s \approx$-classes for $s < r - 1$, then $|C| = \phi(p^r) + \phi(p^{r-1}) + \ldots + \phi(p^{s+1}) = p^r - p^s$.
This is not enough to be able to distinguish the two different types of class and reconstruct the directed power graph from the undirected power graph. For example, we could have a \( \equiv \)-class \( C \) of type (i) (so \( C \) is also a \( \approx \)-class) containing elements of order 13, so that \( |C| = \phi(13) = 12 \) and a \( \equiv \)-class \( D \) of type (ii) which is a union of two \( \approx \)-classes whose elements are of order 16 and 8, so that \( |D| = 2^4 - 2^{3-1} = 16 - 4 = 12 = |C| \). We cannot yet distinguish these two classes from each other, so we need to extract more information from the undirected graph to be able to do this.

**Definition 5.4.** For a set \( S \), the closed neighbourhood of \( S \) is \( \bar{N}(S) = \cap \{ \bar{N}(s) \mid s \in S \} \).

**Lemma 5.3** (1). (i) If \( C \) is a \( \equiv \)-class of type (ii) (as in Corollary 5.2) with \( |C| = p^r - p^s \) for some prime \( p \) and positive integers \( r \) and \( s < r - 1 \), then \( |\bar{N}(\bar{N}(C))| = p^r \).

(ii) If \( C \) is a \( \equiv \)-class and also a \( \approx \)-class, and \( |\bar{N}(\bar{N}(C))| = p^r \) for some prime \( p \) and positive integer \( r \), then \(|C| \neq p^r - p^s \) for any \( s < r - 1 \).

We omit the proof because of space constraints, but there is a proof in [4].

This result means that we can recognise \( \equiv \)-classes of both types from Corollary 5.2 and we can find what orders the elements of each class have.

**Proof of Theorem 5.2** following Cameron’s proof in [4]. Suppose \( G \) and \( H \) are finite groups. It is obvious that if \( \bar{g}(G) \cong \bar{g}(H) \) then \( g(G) \cong g(H) \).

For the converse, we show how to construct \( \bar{g}(G) \) from \( g(G) \). First, if there is more than one vertex in \( g(G) \) adjacent to every other vertex, then by Theorem 5.2 we know \( G \), and therefore we know all of the directional information. So suppose that the identity is the only vertex adjacent to every other graph vertex. Now, partition \( g(G) \) into \( \equiv \)-classes. We know which class is the identity class, so we direct all the edges incident on the identity towards the identity, and then consider non-identity classes. For every non-identity \( \equiv \)-class \( C \), by Lemma 5.3 we can find out how many \( \approx \)-classes \( C \) contains, and the orders of the elements. If \( C \) contains more than one \( \approx \)-class then it has size \( p^r - p^s \) for some \( s < r - 1 \) by Lemma 5.3 and it contains \( \phi(p^k) \) elements of order \( p^k \) for \( k = s + 1, \ldots, r \). Note that we can permute the elements of any \( \equiv \)-class with a graph automorphism, and so we can choose any labelling for \( C \). So we can partition \( C \) into \( r - s \) \( \approx \)-classes by partitioning into sets of sizes \( \phi(p^{s+1}), \phi(p^{s+2}), \ldots, \phi(p^r) \).

Now that we have partitioned \( g(G) \) into \( \approx \)-classes, we can add bi-directional arrows between every pair of vertices in each \( \approx \)-class. If \( A \) and \( B \) are distinct \( \approx \)-classes made up of elements of order \( n \) and \( m \) respectively, and \( \langle B \rangle \leq \langle A \rangle \) (or, equivalently, \( m \mid n \)) then we want edges from every element in \( A \) to every element in \( B \), and otherwise no edges between the elements in the two classes.

If \( m \mid n \), then \( \phi(m) \mid \phi(n) \) with equality only if \( n = 2m \) and \( m \) is odd. So if \( A \) and \( B \) are of different sizes and are connected in \( g(G) \) then we add arrows from every element in \( A \) to every element in \( B \). In the case that \( |A| = |B| \) and the classes are connected, then \( n = 2m \) and \( m \) is odd, so \( \langle A \rangle \) contains an element of order 2 and \( \langle B \rangle \) does not, so we can identity which class is \( A \) because it will be connected to a non-identity singleton class (an element of order 2) and \( B \) will not be. So again, we can add arrows from every element in \( A \) to every element in \( B \), completing the construction of \( \bar{g}(G) \) from \( g(G) \).

**Corollary 5.3.** For \( G \) and \( H \) finite abelian groups, \( g(G) \cong g(H) \) if and only if \( G \cong H \) [5, Theorem 1].

**Proof.** If \( G \cong H \), it is easy to see that \( g(G) \cong g(H) \).

Conversely, if \( g(G) \cong g(H) \) then by Theorem 5.2 \( \bar{g}(G) \cong \bar{g}(H) \) and so by Corollary 5.1 \( G \cong H \).
Concluding remarks

There are many unexplored areas in this topic, so we give some ideas for future work which we did not have space or time to put in this essay.

We have shown that power graphs do not always determine the group. An interesting study would be to find out how many groups there are to each power graph.

We are also interested in which graphs are power graphs of a finite group. We have shown that every non-planar power graph of a finite group contains a copy of $K_5$, so we know that if graph contains $K_{3,3}$ (which is non-planar) but not $K_5$, then it cannot be the power graph of some finite group.

Curtin and Pourgholi [10] show that, among all finite groups of a given order, the cyclic group has the most edges in its power graph. For the directed power graph, the result follows easily from the fact that, among all finite groups of a given order, the sum of the element orders is maximal for the cyclic group, which is proved in [2]. The undirected case is more difficult, but is proved in [10]. It seems natural to ask which groups have the minimum number of edges in their power graphs. We have seen in Theorem [2.5] that, for a finite group $G$ $g(G)$ is a tree if and only if $G$ is of the form $Z_2 \times Z_2 \times \cdots \times Z_2$. It is easy to see that the power graph of $(Z_2)^m$ has a smaller number of edges than a power graph of any other group of order $2^m$, because a tree is a connected graph with the minimum number of edges. It would be interesting to look for neat result for groups of any given order.

References


