Bull. Aust. Math. Soc. **90** (2014), 418–426
doi:10.1017/S0004972714000434

A GROUP SUM INEQUALITY AND ITS APPLICATION TO POWER GRAPHS

BRIAN CURTIN✉ and G. R. POURGHOLI

(Received 1 April 2014; accepted 4 April 2014; first published online 13 June 2014)

Abstract

Let G be a finite group of order n, and let C_n be the cyclic group of order n. For $g \in G$, let $o(g)$ denote the order of g. Let ϕ denote the Euler totient function. We show that $\sum_{g\in C_n} \phi(o(g)) \geq \sum_{g\in G} \phi(o(g))$, with equality if and only if G is isomorphic to C_n. As an application, we show that among all finite groups of a given order, the cyclic group of that order has the maximum number of bidirectional edges in its directed power graph.

2010 *Mathematics subject classification*: primary 20F99; secondary 05C25.

Keywords and phrases: cyclic groups, Euler totient, Sylow subgroups.

1. Introduction

Our main result is a group-theoretic inequality, which we apply to power graphs.

DEFINITION 1.1. Let G be a finite group. For $g \in G$, let $o(g)$ denote the order of g. Let ϕ denote the Euler totient function. Define

$$\phi(G) = \sum_{g\in G} \phi(o(g)). \tag{1.1}$$

THEOREM 1.2 (Main theorem). *Let G be a finite group of order n, and let C_n be the cyclic group of order n. Then*

$$\phi(C_n) \geq \phi(G), \tag{1.2}$$

with equality if and only if G is isomorphic to C_n.

Our motivation for (1.2) lies in our interest in power graphs of finite groups.

DEFINITION 1.3. The *directed power graph* $\overrightarrow{\mathcal{P}}(G)$ of a group G has vertex set G and directed edge set $\overrightarrow{E}(G) = \{(g, h) \mid g, h \in G, h \in \langle g\rangle\backslash\{g\}\}$. The set of *bidirectional edges* of $\overrightarrow{\mathcal{P}}(G)$ is $\overleftrightarrow{E}(G) = \{\{g, h\} \mid (g, h), (h, g) \in \overrightarrow{E}(G)\}$.

Power graphs are among the various graphs related to algebraic structures. They were introduced in [5–8] in connection with groups and semigroups. For more information about power graphs, the reader is referred to the survey [1], which contains a full review of the literature to date.

Counting bidirectional edges in the directed power graph of a group is straightforward. By Definition 1.3, there is a pair of oppositely directed edges between two distinct group elements precisely when they generate the same subgroup. Recall that the number of generators of a cyclic group of order m is $\phi(m)$.

Lemma 1.4. *With reference to Definition 1.1, each $g \in G$ is a vertex in $\phi(\mathrm{o}(g)) - 1$ bidirectional edges of $\overrightarrow{\mathcal{P}}(G)$, and*

$$|\overleftrightarrow{E}(G)| = \frac{1}{2}\sum_{g\in G}(\phi(\mathrm{o}(g)) - 1) = \frac{\phi(G) - |G|}{2}. \tag{1.3}$$

It was shown in [2] that among directed power graphs of groups of a given finite order, that of the cyclic group has the maximum number of edges. In [4], we showed that the same is true for undirected power graphs. In light of Lemma 1.4, Theorem 1.2 is equivalent to the following related result.

Theorem 1.5. *Among all groups of a given finite order, the cyclic group of that order has the maximum number of bidirectional edges in its directed power graph.*

2. A criterion for a normal cyclic Sylow subgroup

We develop a criterion for the existence of a cyclic normal Sylow subgroup. Throughout this section we use the following notation.

Notation 2.1. Let $n > 1$ be an integer. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ for primes $p_1 < p_2 < \cdots < p_k$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_k$. Abbreviate $p = p_k$ and $\alpha = \alpha_k$. Let

$$Q = \prod_{h=1}^{k} \frac{p_h + 1}{p_h - 1}. \tag{2.1}$$

An elementary exercise in the same vein as [3, Exercise 5, page 143] gives two expressions for $\phi(\mathrm{C}_n)$ derived from n (see also [4, Lemma 2.5]).

Lemma 2.2. *With Notation 2.1, let C_n be the cyclic group of order n. Then*

$$\phi(C_n) = \sum_{d|n} \phi(d)^2 = \prod_{h=1}^{k} \frac{p_h^{2\alpha_h}(p_h - 1) + 2}{p_h + 1}. \tag{2.2}$$

Subtracting the 2 from the numerator of each factor of (2.2) gives the lower bound

$$\phi(\mathrm{C}_n) > \frac{n^2}{Q}. \tag{2.3}$$

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

TABLE 1. Some special values of Q.

ℓ	1	2	3	4	5	6	7	8	9
$\nu(\ell)$	2	3	5	7	11	13	17	19	23
$Q(\mathcal{F}_\ell)$	3	6	9	12	72/5	84/5	189/10	21	252/11
$Q(\mathcal{S}_\ell)$	2	9/2	8	54/5	14	81/5	56/3	1134/55	*

When $k \geq 2$, we may write

$$Q = \frac{1}{p_1 - 1}\Big(\frac{p_1 + 1}{p_2 - 1} \cdots \frac{p_{k-2} + 1}{p_{k-1} - 1}\, \frac{p_{k-1} + 1}{p_k - 1}\Big)(p_k + 1). \tag{2.4}$$

Observe that if $(p_{h-1}, p_h) \neq (2, 3)$, then for $2 \leq h \leq k$,

$$\frac{p_{h-1} + 1}{p_h - 1} \leq 1. \tag{2.5}$$

This immediately gives the following lemma.

LEMMA 2.3. *With Notation 2.1, assume n is odd. Then*

$$Q \leq \frac{p + 1}{p_1 - 1}. \tag{2.6}$$

In Table 1 above we record data concerning some sets of primes which require special treatment. Let $\nu(i)$ denote the ith prime number. For each positive integer ℓ, let $\mathcal{F}_\ell = \{\nu(i) \mid 1 \leq i \leq \ell\}$ and $\mathcal{S}_\ell = \{\nu(i) \mid 1 \leq i \leq \ell - 1\} \cup \{\nu(\ell + 1)\}$. Write $Q(\mathcal{X})$ to denote the value of Q when the set of distinct prime factors of n is $\mathcal{X}$.

LEMMA 2.4. *With Notation 2.1, $Q \leq p + 1$ unless $\{p_i \mid 1 \leq i \leq k\} = \mathcal{F}_k$ with $2 \leq k \leq 8$. Moreover, $Q < p$ whenever n is odd.*

PROOF. If n is odd, then by (2.6), $Q \leq (p + 1)/(p_1 - 1) \leq (p + 1)/2 < p$ since $p_1, p \geq 3$. By (2.1), $Q \leq p + 1$ when $k = 1$. Table 1 shows that $Q > p + 1$ when the set of prime divisors of n is $\mathcal{F}_k$ $(2 \leq k \leq 8)$ and that $Q \leq p + 1$ when the set of prime divisors of n is $\mathcal{F}_9$ or $\mathcal{S}_k$ $(1 \leq k \leq 8)$. Suppose that P is a set of primes with maximum element p and $Q(P) \leq p + 1$. If $p' > p$ is a prime, then $Q(P \cup \{p'\}) = Q(P)(p' + 1)/(p' - 1) \leq (p + 1)(p' + 1)/(p' - 1)$. Now $(p + 1)/(p' - 1) \leq 1$ provided $(p, p') \neq (2, 3)$. In any other case, once the inequality is satisfied by an initial subset of prime factors it is satisfied by adding larger prime factors. The result follows. □

It is well known that

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1). \tag{2.7}$$

Immediate consequences include the following:

$$n = \phi(n) \cdot \frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} \cdots \frac{p_k}{p_k - 1}, \tag{2.8}$$

$$a \mid b \Rightarrow \phi(a) \mid \phi(b) \quad (a, b \in \mathbb{Z}^+). \tag{2.9}$$

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

Lemma 2.5. *With Notation 2.1, suppose that $n \neq 2^\alpha$ for any $\alpha \geq 0$. Then*

$$n \geq Q\phi\Big(\frac{n}{p^\alpha}\Big)p^{\alpha-1}, \tag{2.10}$$

with equality if and only if $n = 2^\alpha 3^\beta$ and $\alpha, \beta > 0$.

Proof. If $n = p^\alpha$, then (2.10) becomes $p^\alpha \geq p^{\alpha-1}(p+1)/(p-1)$, which holds strictly since $p \neq 2$. The inequality fails if n is a power of 2. Now suppose that n has at least two distinct prime factors. By (2.1) and (2.8),

$$\frac{n}{Q} = \phi(n)p_1 \frac{p_2}{(p_1+1)}\frac{p_3}{(p_2+1)}\cdots\frac{p}{(p_{k-1}+1)}\frac{1}{(p+1)}.$$

By (2.7), $\phi(n) = \phi(n/p^\alpha)p^{\alpha-1}(p-1)$, so

$$\frac{n}{Q} = \phi\Big(\frac{n}{p^\alpha}\Big)p^{\alpha-1}(p-1)\cdot\frac{p_1}{(p+1)}\Big(\frac{p_2}{(p_1+1)}\frac{p_3}{(p_2+1)}\cdots\frac{p}{(p_{k-1}+1)}\Big).$$

Observe that for $1 \leq h \leq k-1$, $p_{h+1}/(p_h+1) \geq 1$, with equality if and only if $p_h = 2$ and $p_{h+1} = 3$. Thus $n/Q \geq \phi(n/p^\alpha)p^{\alpha-1}(p-1)p_1/(p+1)$, with equality if and only if $k = 2$, $p_1 = 2$ and $p = 3$. Since $p_1 \geq 2$ and $(p-1)/(p+1) \geq \frac{1}{2}$, we have $p_1(p-1)/(p+1) \geq 1$, with equality if and only if $p_1 = 2$ and $p = 3$. Thus (2.10) holds with equality if and only if $n = 2^\alpha 3^\beta$ with $\alpha, \beta > 0$. □

Lemma 2.6. *With Notation 2.1, let G be a finite group of order n, and let $g \in G$. If $n < Q\phi(\mathrm{o}(g))$, then g is not the identity of G except possibly when $n = 2$.*

Proof. Suppose that e is the identity of G, so $\phi(\mathrm{o}(e)) = 1$. Lemma 2.5 and the hypothesis imply that n is a positive power of 2. In this case, $Q\phi(\mathrm{o}(e)) = 3$, which is less than n unless $n = 2$. When $n = 2$, $n < Q\phi(\mathrm{o}(e))$, so the exception is required. □

Lemma 2.7. *With Notation 2.1, let G be a finite group of prime power order $n > 2$, and let $g \in G$. If $n < Q\phi(\mathrm{o}(g))$, then g generates G.*

Proof. Suppose that $n = p^\alpha$. Then $Q = (p+1)/(p-1)$ by definition, and $\mathrm{o}(g) = p^\ell$ for some ℓ $(0 < \ell \leq \alpha)$ by Lagrange's theorem and Lemma 2.6. Now $\phi(\mathrm{o}(g)) = p^{\ell-1}(p-1)$. Thus $Q\phi(\mathrm{o}(g)) = p^{\ell-1}(p+1)$. Now $p^\alpha = n < Q\phi(\mathrm{o}(g)) = p^{\ell-1}(p+1)$. Thus $p^{\alpha-\ell+1} \leq p$, so $\ell \geq \alpha$. In addition $\ell \leq \alpha$, so $\ell = \alpha$. Hence g generates G. □

Lemma 2.8. *With Notation 2.1, let G be a finite group of order $n > 2$, and let $g \in G$. If $n < Q\phi(\mathrm{o}(g))$, then $p^\alpha \mid \mathrm{o}(g)$.*

Proof. If n has just one prime factor, then g generates G by Lemma 2.7, and the result follows. Assume that n has at least two distinct prime factors. By hypothesis and Lemma 2.5,

$$\phi(\mathrm{o}(g)) > \phi\Big(\frac{n}{p^\alpha}\Big)p^{\alpha-1}. \tag{2.11}$$

For the sake of contradiction, suppose that $p^\alpha \nmid \mathrm{o}(g)$, so $\mathrm{o}(g) \mid n/p$. We consider two cases. If $\alpha = 1$, then (2.9) gives $\phi(\mathrm{o}(g)) \mid \phi(n/p)$, contradicting (2.11). If $\alpha \geq 2$,

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

then (2.9) gives $\phi(\mathrm{o}(g)) \mid \phi(n/p^\alpha)p^{\alpha-2}(p-1)$. In this case $\phi(\mathrm{o}(g)) \le \phi(n/p^\alpha)$ $p^{\alpha-2}(p-1)$, contradicting (2.11). We conclude that $p^\alpha \mid \mathrm{o}(g)$, as required. □

Lemma 2.9. *With Notation 2.1, let G be a finite group of order n, and let $g \in G$. If $\mathrm{o}(g)$ is even and $n < Q\phi(\mathrm{o}(g))$, then $n/\mathrm{o}(g) < p$.*

Proof. Observe that $\mathrm{o}(g) \ge 2\phi(\mathrm{o}(g))$ and $p_1 = 2$, so $n/\mathrm{o}(g) \le n/2\phi(\mathrm{o}(g)) < Q/2$. If $n = 2$, the result is trivial. If $n = 2^\alpha$ for some $\alpha > 1$, then $\mathrm{o}(g) = n$ by Lemma 2.7, so the result follows. Assume n has at least one prime factor other than 2. Then by (2.4), $Q/2 \le 3(p+1)/2(p_2-1)$. Since $p_2 \ge 3$, the right-hand side is at most p, and the result follows. □

Theorem 2.10. *With Notation 2.1, let G be a finite group of order n. Suppose that there exists a non-identity element $g \in G$ such that $n < Q\phi(\mathrm{o}(g))$. Then there is a normal (and hence unique) Sylow p-subgroup of G. Moreover, the Sylow p-subgroup is contained in $\langle g\rangle$ and hence is cyclic.*

Proof. The result is trivial if $n = 2$. If $n > 2$ is a prime power, then the result follows from Lemma 2.7, so assume that n is not a prime power. First suppose that $n/\mathrm{o}(g) < p+1$. Then $|G : \langle g\rangle| = n/\mathrm{o}(g) < p+1$. By Lemma 2.8, $p^\alpha \mid \mathrm{o}(g)$, so $p \nmid |G : \langle g\rangle|$. Thus $\langle g\rangle$ contains a Sylow p-subgroup P of G (which is necessarily cyclic since $\langle g\rangle$ is). Clearly $\langle g\rangle \subseteq C_G(P) \subseteq N_G(P)$, so $|G : N_G(P)| < p+1$. But $|G : N_G(P)|$ is the number of Sylow p-subgroups and must be congruent to 1 modulo p. Thus, it must be the case that there is exactly one Sylow p-subgroup, which is necessarily normal.

Now suppose that $n/\mathrm{o}(g) \ge p+1$. Note that $n/\mathrm{o}(g) < n/\phi(\mathrm{o}(g)) < Q$. Thus by Lemmas 2.4 and 2.9, the following hold: $2 \le k \le 8$, $n = \prod_{i=1}^{k} \nu(i)^{\alpha_i}$ with $\alpha_i \ne 0$ $(1 \le i \le k)$, and $\mathrm{o}(g)$ is odd. In Table 2, we show that other than $n = 2\cdot 3\cdot 5^\alpha$, none of the remaining cases satisfy $n/\phi(\mathrm{o}(g)) < Q$, and thus are not subject to this theorem. In this table, for $2 \le k \le 8$ we mark with a bullet (•) the even integers that are at least $\nu(k)+1$ and strictly less than Q (from Table 1) as the possible values of $n/\mathrm{o}(g)$. Also by Lemma 2.8, $\nu(k)^{\alpha_k} \mid \mathrm{o}(g)$, so $\nu(k) \nmid n/\mathrm{o}(g)$. Since $\mathrm{o}(g)$ is odd, $2^{\alpha_1} \mid n/\mathrm{o}(g)$, where α_1 is the largest power of 2 dividing $n/\mathrm{o}(g)$. It is now easy to read $\mathrm{o}(g)$. The value of $\phi(\mathrm{o}(g))$ will depend upon which primes appear in $\mathrm{o}(g)$, but otherwise is straightforward to compute. All cases other than $n = 2\cdot 3\cdot 5^\alpha$ violate $n/\phi(\mathrm{o}(g)) < Q$.

Suppose that $n = 2\cdot 3\cdot 5^\alpha$. Observe that $\mathrm{o}(g) = 5^\alpha$, so $\langle g\rangle$ is a cyclic Sylow 5-subgroup. Since the order of G is twice an odd number, G contains a subgroup H of index 2. (See [9, Exercise 205] or use Burnside's normal p-complement theorem [9, Theorem 10.21].) Note that H is normal and has order $3\cdot 5^\alpha$. Elementary Sylow arguments give that there is a unique Sylow 5-subgroup P of H. Now P is characteristic in H, and hence normal in G. Since P is the unique Sylow 5-subgroup of G, we have $P = \langle g\rangle$. Thus the theorem holds in this case. □

The contrapositive form of Theorem 2.10 is interesting.

Corollary 2.11. *With Notation 2.1, let G be a finite group of order n, and let p be the largest prime divisor of n. If there is more than one Sylow p-subgroup, then $n \ge Q\phi(\mathrm{o}(g))$ for all $g \in G$.*

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

Table 2. Exceptional cases in the proof of Theorem 2.10.

k	$\nu(k)$ • $\dfrac{n}{\mathrm{o}(g)}$	Q α_1 case	$\mathrm{o}(g)$ $\phi(\mathrm{o}(g))$	$\left\lfloor \dfrac{n}{\phi(\mathrm{o}(g))} \right\rfloor$
2	3	6		
	• 4	2	3^{α_1}	
		all	$2 \cdot 3^{\alpha_1-1}$	$6 = Q$
3	5	9		
	• 6	1	$3^{\alpha_2-1}5^{\alpha_3}$	
		$\alpha_2 = 1$	$4 \cdot 5^{\alpha_3-1}$	**7.5** $< Q$
		$\alpha_2 > 1$	$2 \cdot 3^{\alpha_2-2}4 \cdot 5^{\alpha_3-1}$	$11 > Q$
	• 8	3	$3^{\alpha_2}5^{\alpha_3}$	
		all	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}$	$15 > Q$
4	7	12		
	• 8	3	$3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}$	
		all	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1}$	$17 > Q$
	• 10	1	$3^{\alpha_2}5^{\alpha_3-1}7^{\alpha_4}$	
		$\alpha_3 = 1$	$2 \cdot 3^{\alpha_2-1}6 \cdot 7^{\alpha_4-1}$	$14 > Q$
		$\alpha_3 > 1$	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-2}6 \cdot 7^{\alpha_4-1}$	$21 > Q$
5	11	14.4		
	• 12	2	$3^{\alpha_2-1}5^{\alpha_3}7^{\alpha_4}11^{\alpha_5}$	
		$\alpha_2 = 1$	$4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4}10 \cdot 11^{\alpha_5-1}$	$19 > Q$
		$\alpha_2 > 1$	$2 \cdot 3^{\alpha_2-2}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1}10 \cdot 11^{\alpha_5-1}$	$28 > Q$
	• 14	1	$3^{\alpha_2}5^{\alpha_3}7^{\alpha_4-1}11^{\alpha_5}$	
		$\alpha_4 = 1$	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}10 \cdot 11^{\alpha_5-1}$	$28 > Q$
		$\alpha_4 > 1$	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1}10 \cdot 11^{\alpha_5-1}$	$33 > Q$
6	13	16.8		
	• 14	1	$3^{\alpha_2}5^{\alpha_3}7^{\alpha_4-1}11^{\alpha_5}13^{\alpha_6}$	
		$\alpha_4 = 1$	$2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}10 \cdot 11^{\alpha_5-1}12 \cdot 13^{\alpha_6-1}$	$31 > Q$
		$\alpha_4 > 1$	$\begin{cases} 2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-2} \\ \times 10 \cdot 11^{\alpha_5-1}12 \cdot 13^{\alpha_6-1} \end{cases}$	$36 > Q$
	• 16	4	$3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}11^{\alpha_5}13^{\alpha_6}$	
		all	$\begin{cases} 2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1} \\ \times 10 \cdot 11^{\alpha_5-1}12 \cdot 13^{\alpha_6-1} \end{cases}$	$41 > Q$
7	17	18.9		
	• 18	1	$3^{\alpha_2-2}5^{\alpha_3}7^{\alpha_4}11^{\alpha_5}13^{\alpha_6}17^{\alpha_7}$	
		$\alpha_2 = 2$	$\begin{cases} 4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1}10 \cdot 11^{\alpha_5-1} \\ \times 12 \cdot 13^{\alpha_6-1}16 \cdot 17^{\alpha_7-1} \end{cases}$	$33 > Q$
		$\alpha_2 > 2$	$\begin{cases} 2 \cdot 3^{\alpha_2-3}4 \cdot 5^{\alpha_3-1}6 \cdot 7^{\alpha_4-1} \\ \times 10 \cdot 11^{\alpha_5-1}12 \cdot 13^{\alpha_6-1}16 \cdot 17^{\alpha_7-1} \end{cases}$	$49 > Q$
8	19	21		
	• 20	2	$3^{\alpha_2}5^{\alpha_3-1}7^{\alpha_4}11^{\alpha_5}13^{\alpha_6}17^{\alpha_7}19^{\alpha_8}$	
		$\alpha_3 = 1$	$\begin{cases} 2 \cdot 3^{\alpha_2-1}6 \cdot 7^{\alpha_4-1}10 \cdot 11^{\alpha_5-1} \\ \times 12 \cdot 13^{\alpha_6-1}16 \cdot 17^{\alpha_7-1}18 \cdot 19^{\alpha_8-1} \end{cases}$	$46 > Q$
		$\alpha_3 > 1$	$\begin{cases} 2 \cdot 3^{\alpha_2-1}4 \cdot 5^{\alpha_3-2}6 \cdot 7^{\alpha_4-1}10 \cdot 11^{\alpha_5-1} \\ \times 12 \cdot 13^{\alpha_6-1}16 \cdot 17^{\alpha_7-1}18 \cdot 19^{\alpha_8-1} \end{cases}$	$58 > Q$

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

The bound in Theorem 2.10 is tight in the following sense. In the alternating group $\mathbb{A}_4$, $n = 12$, $Q = 6$, and elements have order 3, 2, and 1. For $g \in \mathbb{A}_4$ with $\mathrm{o}(g) = 3$, $\phi(\mathrm{o}(g)) = 2$. Thus $n = Q\phi(\mathrm{o}(g))$. However, $\mathbb{A}_4$ has four Sylow 3-subgroups, which happen to be cyclic.

3. Proof of the main theorem

To prove Theorem 1.5, we need some facts about direct and semi-direct products.

Lemma 3.1. *Let U and T be finite groups, and let $G = U \times T$ be the direct product of U and T. Then $\phi(G) \le \phi(U)\phi(T)$. Moreover, if $(|U|, |T|) = 1$, then $\phi(G) = \phi(U)\phi(T)$.*

Proof. Given $g = (u, t) \in G$, $\mathrm{o}(g) = \mathrm{o}(u)\mathrm{o}(t)/(\mathrm{o}(u), \mathrm{o}(t))$. Thus by the multiplicative property of the totient function and by (2.9),

$$\phi(\mathrm{o}(g)) = \phi\Big(\frac{\mathrm{o}(u)}{(\mathrm{o}(u), \mathrm{o}(t))}\Big)\phi(\mathrm{o}(t)) \le \phi(\mathrm{o}(u))\phi(\mathrm{o}(t)).$$

Now

$$\begin{aligned} \phi(G) &= \sum_{u\in U}\sum_{t\in T}\phi(\mathrm{o}(u,t)) = \sum_{u\in U}\sum_{t\in T}\phi\Big(\frac{\mathrm{o}(u)}{(\mathrm{o}(u), \mathrm{o}(t))}\Big)\phi(\mathrm{o}(t)) \\ &\le \sum_{u\in U}\phi(\mathrm{o}(u))\sum_{t\in T}\phi(\mathrm{o}(t)) = \phi(U)\phi(T). \end{aligned} \tag{3.1}$$

Observe that if $(|U|, |T|) = 1$, then $(\mathrm{o}(u), \mathrm{o}(v)) = 1$ for all $u \in U$ and $t \in T$, so equality holds throughout. □

The condition $(|U|, |T|) = 1$ in Lemma 3.1 can be replaced with other conditions to reach the same conclusion. If U is an elementary abelian 2-group, then all elements of U have order 1 or 2. The totient of these numbers and their divisors is 1, so $\phi(\mathrm{o}(u)) = \phi(\mathrm{o}(u)/(\mathrm{o}(u), \mathrm{o}(t))) = 1$ for all $u \in U$ and $t \in T$. Now (3.1) gives $\phi(G) = \phi(U)\phi(T)$. Similarly, if $(|U|, |T|) = 2$ and $|U|$ is twice an odd number, then $\phi(\mathrm{o}(u)) = \phi(\mathrm{o}(u)/(\mathrm{o}(u), \mathrm{o}(t)))$, so $\phi(G) = \phi(U)\phi(T)$.

Lemma 3.2 [4, Lemma 5.3]. *Suppose that G is a finite group and that $G = U \rtimes_\varphi V$ is the semidirect product of a normal abelian subgroup U and a subgroup V. Assume that U and V have coprime orders. Then $\mathrm{o}_G(uv) \mid \mathrm{o}_{U\times V}(uv)$ for all $u \in U$ and $v \in V$.*

Corollary 3.3. *With reference to Lemma 3.2, $\phi(\mathrm{o}_G(uv)) \mid \phi(\mathrm{o}_{U\times V}(uv))$, and $\phi(U \rtimes_\varphi V) \le \phi(U \times V)$.*

Proof. The divisibility follows from Lemma 3.2 and (2.9), and the inequality follows from (1.1). □

Theorem 3.4 [9, Theorem 10.30]. *(Schur–Zassenhaus theorem) Let G be a finite group, and let K be a normal subgroup of G with $(|K|, |G : K|) = 1$. Then G is a semidirect product of K and G/K. In particular, there exists a subgroup H of G with order $|G : K|$ such that $G = K \rtimes_\varphi H$ for some homomorphism $\varphi : H \to \mathrm{Aut}(K)$.*

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

Before treating the general case we present a special case involving cyclic groups.

LEMMA 3.5. *Let a and b be coprime positive integers. Then* $\phi(C_a \rtimes_\varphi C_b) \leq \phi(C_a \times C_b)$*, with equality if and only if the semi-direct product is direct.*

PROOF. Note that $G = \mathrm{C}_a \rtimes_\varphi \mathrm{C}_b$ and $H = \mathrm{C}_a \times \mathrm{C}_b \cong \mathrm{C}_{ab}$ are defined on the cartesian product of the underlying sets of C_a and C_b. Let $n = ab$. By Corollary 3.3, $\phi(\mathrm{o}_G(g)) | \phi(\mathrm{o}_H(g))$ for all $g \in G$. Thus $\sum_{g\in G} \phi(\mathrm{o}_G(g)) \leq \sum_{g\in G} \phi(\mathrm{o}_H(g))$. Moreover, equality holds if and only if $\phi(\mathrm{o}_G(g)) = \phi(\mathrm{o}_H(g))$ for all $g \in G$.

Suppose equality holds for the sums. Pick a generator h of H. We are done if $\mathrm{o}_G(h) = n$ since $G \cong \mathrm{C}_n \cong H$ in this case. Suppose for the sake of contradiction that $\mathrm{o}_G(h) \neq n$. Now $\mathrm{o}_G(h)|n$, so in light of (2.9), $m = \mathrm{o}_G(h) = n/2$ is odd. Let $L = \langle h\rangle \subset G$, so $|L|$ is odd and $|G : L| = 2$. This implies $L \lhd G$. Let K be a Sylow 2-subgroup of G, so $|K| = 2$. Now $G = LK$ and $L \cap K = \{e\}$, where e is the identity of G. Hence G is the semi-direct product $G = L \rtimes_\psi K$ (see [9, Theorem 9.13]). Hence G is isomorphic to the semi-direct product $\mathrm{C}_m \rtimes_\psi \mathrm{C}_2$. Since C_m is normal in G, we have that $(uv)^2 \in \mathrm{C}_m$ for all $u \in \mathrm{C}_m$, $v \in \mathrm{C}_2$. In particular, $\mathrm{o}_G(uv)$ is even. However, $\mathrm{o}_G(uv) \neq 2m$ since G is not cyclic. Now $\phi(\mathrm{o}_G(uv)) < \phi(2m) = \phi(n)$, since $\mathrm{o}(u)|m$. This implies $\phi(G) < \phi(\mathrm{C}_n)$, contrary to our assumption. Thus G is cyclic as required. □

We are ready to prove our main result, namely that $\phi(\mathrm{C}_n) \geq \phi(G)$, with equality if and only if G is isomorphic to C_n.

PROOF OF THEOREM 1.2. The result is clear for $n \in \{1, 2\}$, so assume that $n \geq 3$. Suppose that $\phi(G) \geq \phi(\mathrm{C}_n)$. For some $g \in G$, $\phi(\mathrm{o}(g))$ is at least the average value over the group, so $\phi(\mathrm{o}(g)) \geq \phi(G)/n \geq \phi(\mathrm{C}_n)/n > n/Q$ by (2.3).

We proceed by induction on the number of distinct prime factors of n. If $|G|$ has just one prime factor, then G is cyclic by Lemma 2.7, and hence isomorphic to C_n. Now assume that for all n' with fewer distinct prime factors than n and for all groups G' of order n', we have $\phi(\mathrm{C}_{n'}) \geq \phi(G')$, with equality if and only if G' is isomorphic to $\mathrm{C}_{n'}$.

By Theorem 2.10, there exists a Sylow p-subgroup P of G which is both cyclic and normal, where p is the largest prime divisor of n. Since P is a Sylow p-subgroup, $|G : P|$ is coprime to $|P|$. Abbreviate $a = |P|$, $b = |G : P|$. By Theorem 3.4, $G = P \rtimes_\varphi T$ for some subgroup $T \subseteq G$ with order b and some homomorphism $\varphi : T \to \mathrm{Aut}(P)$.

Since P is cyclic, Corollary 3.3 gives that $\phi(G) = \phi(P \rtimes_\varphi T) \leq \phi(P \times T)$. But by Lemma 3.1, $\phi(P \times T) = \phi(P)\phi(T)$. Identify C_n with the direct product of cyclic subgroups $\mathrm{C}_a \times \mathrm{C}_b$. Observe that $\phi(\mathrm{C}_n) = \phi(\mathrm{C}_a)\phi(\mathrm{C}_b)$ by Lemma 3.1 and $\phi(\mathrm{C}_a) = \phi(P)$ since both are cyclic and of the same order.

Note that $p \nmid |T| = b$ by construction and $|T|\,|n$ by Lagrange's theorem, so $|T|$ has fewer distinct prime divisors than n and $|T| < n$. By the induction hypothesis $\phi(\mathrm{C}_b) \geq \phi(T)$, with equality if and only if T is cyclic. Thus $\phi(G) \leq \phi(\mathrm{C}_n)$, with equality only if T is cyclic. By assumption $\phi(G) \geq \phi(\mathrm{C}_n)$, hence $\phi(G) = \phi(\mathrm{C}_n)$ and T is cyclic of order b. Thus G is isomorphic to $\mathrm{C}_a \rtimes_\varphi \mathrm{C}_b$. The result follows by Lemma 3.5. □

PROOF OF THEOREM 1.5. Straightforward from Theorem 1.2 and (1.3). □

https://doi.org/10.1017/S0004972714000434 Published online by Cambridge University Press

Theorem 1.2 implies that C_n is determined up to isomorphism by $\phi(C_n)$. However, $\phi(G)$ depends only upon the orders of its elements, and does not determine G in general. Indeed, $\phi(C_4 \times C_4) = \phi(C_2 \times Q) = 28$, where Q is the quaternion group, since each has three elements of order 2 and 12 of order 4. We pose a related question. Let G and H be finite groups of the same order with $\phi(G) = \phi(H)$. Suppose that G is simple. Is H necessarily simple?

References

[1] J. Abawajy, A. Kelarev and M. Chowdhury, 'Power graphs: a survey', *Electron. J. Graph Theory Appl.* **1**(2) (2013), 125–147.

[2] H. Amiri, S. M. Jafarian Amiri and I. M. Isaacs, 'Sums of element orders in finite groups', *Comm. Algebra* **37**(9) (2009), 2978–2980.

[3] D. M. Burton, *Elementary Number Theory*, 5th edn (McGraw-Hill, Boston, MA, 2002).

[4] B. Curtin and G. R. Pourgholi, 'Edge-maximality of power graphs of finite cyclic groups', *J. Algebraic Combin.*, to appear. Online first edition doi: 10.1007/s10801-013-0490-5; arXiv:1311.2984.

[5] A. V. Kelarev and S. J. Quinn, 'A combinatorial property and power graphs of groups', in: *Contributions to General Algebra, 12 (Vienna, 1999)* (Heyn, Klagenfurt, 2000), 229–235.

[6] A. V. Kelarev and S. J. Quinn, 'Directed graph and combinatorial properties of semigroups', *J. Algebra* **251**(1) (2002), 16–26.

[7] A. V. Kelarev and S. J. Quinn, 'A combinatorial property and power graphs of semigroups', *Comment. Math. Univ. Carolin.* **45** (2004), 1–7.

[8] A. V. Kelarev, S. J. Quinn and R. Smolikova, 'Power graphs and semigroups of matrices', *Bull. Aust. Math. Soc.* **63**(2) (2001), 341–344.

[9] J. S. Rose, *A Course on Group Theory* (Dover Publications, New York, 1994).

BRIAN CURTIN, Department of Mathematics and Statistics,
University of South Florida, Tampa,
FL 33620, USA
e-mail: bcurtin@usf.edu

G. R. POURGHOLI, School of Mathematics,
Statistics and Computer Science, University of Tehran,
Tehran 14155-6455, Iran
e-mail: pourgholi@ut.ac.ir