Irish Math. Soc. Bulletin
Number 84, Winter 2019, 21–24
ISSN 0791-5578

On the order of a smallest group with a given representation degree

ROBERT HEFFERNAN AND DESMOND MACHALE

Abstract. We consider the problem of finding the minimal order of a finite group G that has an irreducible complex representation of degree n for small values of n.

It is well known that every finite group G with $k(G)$ conjugacy classes has $k(G)$ inequivalent irreducible complex matrix representations of degrees d_i, $1 \leq i \leq k(G)$, and that the degree equation

$$\sum_{i=1}^{k(G)} d_i^2 = |G|$$

holds [3, Cor. 2.7]. In this note we ask the question: For each n, what is the order $f(n)$ of a smallest group G with an irreducible complex representation of degree n?

For small n, the answer is provided by the following table:

n	1	2	3	4	5	6	7	8	9	10
$f(n)$	1	6	12	20	55	42	56	72	144	110
n	11	12	13	14	15	16	17	18	19	20
$f(n)$	253	156	351	336	240	272	1751	342	3420	500
n	21	22	23	24	25	26	27	28	29	30
$f(n)$	672	506	1081	600	2525	702	1512	812	1711	930
n	31	32								
$f(n)$	992	1440								

The purpose of this note is to discuss and justify the entries in this table. For very small values of n we can proceed by hand but, as n increases, more theory is needed. As n becomes larger, we make extensive use of the Small Groups library, which we access using GAP [1].

It is well known that each d_i is a divisor of $|G|$ [3, Thm. 3.11], and the number of d_i equal to 1 is precisely $|G : G'|$, the index of the commutator subgroup of G [3, Cor. 2.23]. Moreover, if A is an abelian normal subgroup of G, then $d_i \leq |G : A|$ [3, Thm. 6.15].

If $n = 1$, then the answer is clearly the trivial cyclic group C_1. So $f(1) = 1$.

From now on all the groups we consider are nonabelian, since for all abelian groups, $d_i = 1$ for all i.

If $n = 2$, then since d_i divides $|G|$ and $\sum d_i^2 = |G|$, we have $|G| \geq 2^2 + 2 = 6$. Luckily, there is a nonabelian group of order 6, S_3, with degree equation

$$6 = 1^2 + 1^2 + 2^2,$$

and so S_3 has an irreducible representation of degree 2. S_3 is the unique nonabelian group of order 6 with this property. So $f(2) = 6$.

In general we can say that $f(n) \geq n^2 + n$ as $f(n)$ is a multiple of n, $n^2 < f(n)$ and G has a trivial degree $d_1 = 1$.

2010 *Mathematics Subject Classification.* 20D99, 20C15.
Key words and phrases. Groups, Representations, Degrees.
Received on 15-11-2019, revised 8-1-2020.

Next, consider $n = 3$. We know that $f(3) \geq 3^2 + 3 = 12$ and among the groups of order 12 there is just one, A_4, with degree equation

$$12 = 1^2 + 1^2 + 1^2 + 3^2.$$

So, $f(3) = 12$.

If $n = 4$, then $f(4) \geq 4^2 + 4 = 20$, and there is a unique group of order 20, namely $\mathrm{Hol}(C_5)$, with degree equation

$$20 = 1^2 + 1^2 + 1^2 + 1^2 + 4^2$$

and so $f(4) = 20$.

If $n = 5$, then $f(5) \geq 5^2 + 5 = 30$. But every group of order 30 has a normal subgroup of order 15, which is abelian, so $d_i \leq \frac{30}{15} = 2$ for all i. However, 5 divides the minimal $|G|$, so

$$|G| = 35, 40, 45, 50, 55, 60, \cdots$$

Now, Sylow theory easily gives that groups of order 35 and 45 are abelian, so

$$|G| = 40, 50, 55, 60, \cdots .$$

Diophantine analysis can be used to rule out 40 and 50; For example, if $40 = \sum d_i^2 + 5^2$, we can have only one representation of degree 5, and none of degree 4, since $25 + 16 = 41 > 40$. Thus the other representations are of degrees 1 or 2, the only allowable divisors of 40. Thus the degree equation becomes

$$x + 4y + 25 = 40$$

or

$$x + 4y = 15,$$

which turns out to have no viable solutions, given that d_i must divide 40. Similarly, every group of order 50 has an abelian subgroup of order 25 and index 2, which forces d_i to be at most 2, for all i. So, 50 is ruled out as a possibility.

Now consider in general the case where $p < q$ are odd primes and p divides $q - 1$. It is well known that in this case there is a unique nonabelian group G of order pq which has $k(G) = p + \frac{q-1}{p}$ conjugacy classes, and $|G : G'| = p$. The degree equation of this group is easily seen to be

$$pq = p + \left[\frac{q-1}{p}\right] p^2,$$

and G has a representation of degree p. This gives in general an upper bound for $f(p)$ where p is an odd prime: find a prime q with p dividing $q - 1$. Then $f(p) \leq pq$. So we see finally that $f(5) = 55$. In like manner we find that $f(11) = 11 \cdot 23 = 253$.

In fact, according to James and Liebeck [4], we have the following: let q be a prime and let p divide $q - 1$, where p is not necessarily a prime, and let $r = (q - 1)/p$. Then there is a group G of order qp with $|G : G'| = p$ and $k(G) = p + r$ with r irreducible representations of degree p. So, $f(p) \leq qp$.

If $n = 6$, then $f(6) \geq 6^2 + 6 = 42$. Luckily, there is a unique group of order 42 with degree equation

$$42 = 6 \cdot 1^2 + 6^2,$$

which has a representation of degree 6. So $f(6) = 42$.

Notice that $f(5) = 55 > 42 = f(6)$, so that the function $f(n)$ is not in general increasing.

If $n = 7$, then $f(7) \geq 7^2 + 7 = 56$ and there is a group of order 56 with degree equation

$$56 = 7 \cdot 1^2 + 7^2$$

and so $f(7) = 56$.

If $n = 8$, then $f(8) \geq 8^2 + 8 = 72$ and there is a group of order 72 with an irreducible representation of degree 8. So, $f(8) = 72$.

Now we introduce some heavier machinery. See Sloane's integer sequence A220470 [2] for details.

(i) $f(n) = n^2 + n$ if and only if $n + 1$ is a prime or a power of a prime. This is consistent with the results above and means we can write down the values of $f(n)$ for $n = 10, 12, 15, 16, 18, 22, 24, 26, 28, 30$ and 31. See Harden [2].

(ii) An upper bound for $f(n)$ in general is given by nq^n where q^n is the smallest prime power which is congruent to 1 modulo n. This is because the group of affine transformations $x \mapsto ax + b$ from the finite field $\mathrm{GF}(q^n)$ to itself, where $a^n = 1$ and b is an arbitrary element of $\mathrm{GF}(q^n)$, has order nq^n and has a representation of degree n.

(iii) $f(n)$ is a sub-multiplicative function, i.e. $f(ab) \leq f(a)f(b)$ because if A has a representation of degree a and B has a representation of degree b, then $A \times B$ has a representation of degree ab.

Now, if $n = 9$, then since 10 is not a prime power, $f(9) > 9^2 + 9 = 90$. By the above, $f(9) \leq f(3)f(3) = 12 \cdot 12 = 144$. GAP can be used to rule out values of $|G|$ between 90 and 144, so $f(9) = 144$. We again note that $f(9) = 144 > 110 = f(10)$. Indeed, there are infinitely many instances of this phenomenon.

The remaining values in the table can be filled in using GAP, but the values for $n = 17$ and $n = 19$ have also been derived by Harden [2] using representation theory and extensive non-trivial calculations.

To find values of $f(n)$ using GAP we can simply search through nonabelian groups in the Small Groups library whose orders are multiples of n greater than or equal to $n^2 + n$ looking for a group with a character of degree n. For small n this works reasonably well but in some cases, such as $n = 32$, the large number of groups to be considered becomes an issue. For instance, there are 1,060,391 nonabelian groups of order 1280 and we must compute the character degrees of each of these in turn to rule out 1280 as a possible value for $f(32)$. This computation does not take long for an individual group, but when such a large number of groups must be checked this approach is impractical. However, an elementary result in character theory [3, Cor. 2.30] says that $d_i^2 \leq |G : Z(G)|$ and so, in particular, $n^2 \leq |G : Z(G)|$. Checking this condition for a given group G is generally much quicker than computing the character degrees, allowing us to find $f(32)$ in a reasonable amount of time. We know that $f(32) \geq 32^2 + 32 = 1056$ and, by (iii) above, we can also say $f(32) \leq f(4)f(8) = 20 \cdot 72 = 1440$. We can now inspect orders that are multiples of 32 between these two bounds to find that $f(32) = 1440$.

We note that there exist n for which two or more groups realise $f(n)$. For example, small groups 72/39 and 72/41 both have a representation of degree 8. Other examples occur for $n = 20, 21, 24$ and 32.

The result that if $n + 1$ is prime or a prime power then $f(n) = n(n + 1)$, has some interesting connections with several difficult and unsolved problems in number theory:

(a) Sophie Germain primes. If p is a prime such that $2p+1$ is also prime, then $f(2p) = 2p(2p + 1)$. Since $f(2p) \leq f(2)f(p) = 6f(p)$, we have $p(2p + 1)/3 \leq f(p)$.

(b) Mersenne primes. If p is a prime such that $2^p - 1$ is also prime, then $f(2^p - 1) = (2^p - 1)(2^p)$. In fact in general, $f(2^n - 1) = (2^n - 1)(2^n)$.

(c) Fermat primes. If $2^n + 1$ is prime, it is known that $n = 2^k$, for some natural number k. Then $f(2^n) = (2^n)(2^n + 1)$.

We conclude with a number of questions:

(1) Is it possible to have $f(a) = f(b)$ for different values of a and b?

(2) Can we have arbitrarily long sequences where $f(n)$ is decreasing?

(3) Are there infinitely many primes p for which $f(p) = pq$, where q is the smallest prime such that p divides $q-1$? We note that many of the values of $f(n)$ which we have found arise from Frobenius groups, such as these groups of order pq. However, we do not know of any conceptual reason why this should be the case
(4) Is it true that a smallest group with a representation of degree n, will always have trivial centre? This is true for all the cases we have presented.

Some of the results in this paper were presented at the Munster Groups conference held at UCC, Cork in September 2018.

References

[1] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.2*, 2019.
[2] David L. Harden. The on-line encyclopedia of integer sequences, Sequence A220470. `https://oeis.org/A220470`.
[3] I. M. Isaacs. *Character theory of finite groups*. Academic Press, New York, 1976.
[4] Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2001.

(Robert Heffernan) Department of Mathematics, Cork Institute of Technology

(Desmond MacHale) School of Mathematical Sciences, University College Cork
E-mail address, R. Heffernan: `robert.heffernan@cit.ie`
E-mail address, D. MacHale: `d.machale@ucc.ie`