Hart, Sarah and Mcveagh, Dan (2020) Groups with many roots. International Journal of Group Theory , ISSN 2251-7650. (In Press)

www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (20xx), pp. xx-xx.

www.ui.ac.ir

GROUPS WITH MANY ROOTS

SARAH B. HART* AND DANIEL MCVEAGH

Communicated by Gunnar Traustason

Abstract. Given a prime p, a finite group G and a non-identity element g, what is the largest number of p^{th} roots g can have? We write $\varrho_p(G)$, or just ϱ_p, for the maximum value of $\frac{1}{|G|}|\{x \in G : x^p = g\}|$, where g ranges over the non-identity elements of G. This paper studies groups for which ϱ_p is large. If there is an element g of G with more p^{th} roots than the identity, then we show $\varrho_p(G) \leq \varrho_p(P)$, where P is any Sylow p-subgroup of G, meaning that we can often reduce to the case where G is a p-group. We show that if G is a regular p-group, then $\varrho_p(G) \leq \frac{1}{p}$, while if G is a p-group of maximal class, then $\varrho_p(G) \leq \frac{1}{p} + \frac{1}{p^2}$ (both these bounds are sharp). We classify the groups with high values of ϱ_2, and give partial results on groups with high values of ϱ_3.

1. Introduction

Let g be an element of a finite group G, and let p be prime. How many p^{th} roots can g have in G? If we allow $g = 1$, then the answer is $|G|$, and this will occur precisely when the group has exponent p. There have been several results giving lower bounds for the number of solutions of $x^p = g$ in a finite group G, where g is any element of G that has at least one p^{th} root. For the case $g = 1$, a classical result of Kulakov states that if G is a non-cyclic p-group of order p^n, where p is odd, then the number of solutions of the equation $x^p = 1$ in G is divisible by p^2. (This follows from the fact that the number of subgroups of order p is congruent to 1 modulo p^2 – see for example [6, III, Satz 8.8] for a more modern proof.) This was later improved by Berkovich to show that if G is a finite p-group which is not metacyclic, and if $p > 3$, then the number of solutions of $x^p = 1$ in G is divisible by p^3 (see [6, III, Satz 11.8]). Blackburn [3] showed further that if G is an irregular p-group that is not of maximal

MSC(2010): Primary: 20D15; Secondary: 20F99.
Keywords: p^{th} roots, square roots, cube roots.
Received: 30 October 2019, Accepted: 27 February 2020.
∗Corresponding author.
http://dx.doi.org/10.22108/ijgt.2020.119870.1582

.

class, then the number of solutions of $x^p = 1$ is divisible by p^p. Later, Lam [9] generalised the problem to consider the number of solutions of $x^{p^k} = g$, where g is any element of a finite group G, p is prime and k is a positive integer. He showed that if G is a finite non-cyclic p-group, where p is odd, then the number of solutions of $x^{p^k} = g$ in G is divisible by p^2. Berkovich [2] improved this result as follows. Let G be a finite p-group that is neither cyclic nor a 2-group of maximal class, and let $k \geq 1$. If g is an element of G such that $\exp(G) \geq p^k|\langle g\rangle|$, then the number of solutions in G of $x^{p^k} = g$ is divisible by p^{k+1}. In particular, if G is not cyclic or a 2-group of maximal class, then those non-identity elements which do have p^{th} roots each have at least p^2 of them. Our interest, in this paper, will be finding upper bounds for the number of p^{th} roots that a non-identity element can have. More specifically, we investigate upper bounds for the proportion of elements of a finite group G that can be p^{th} roots of a single non-identity element. Before describing our results in more detail, we introduce some notation.

Notation 1.1. Let G be a finite group and p a prime. For any g in G, let $R_p(g) = \{x \in G : x^p = g\}$. Let $\varrho_p(G) = \frac{1}{|G|}\max_{g\in G\setminus\{1\}}\{|R_p(G)|\}$. We write R_p and ϱ_p, $R(g)$ and $\varrho(G)$, or simply R and ϱ, whenever g, G or p are clear from context. We will refer to $\varrho(G)$ as the *rootiness* or p^{th}-*rootiness* of G. We will call g a *rooty element* if $\varrho(G) = \frac{|R(g)|}{|G|}$.

In Section 2 we obtain some general results about p^{th}-rootiness. We will show in Lemma 2.6 that if there is an element of a group G that has more p^{th} roots than the identity, then the rootiness of G cannot exceed that of its Sylow p-subgroups. It therefore makes sense to concentrate mainly on p-groups. We show (Proposition 2.9) that if G is a regular p-group, then $\varrho(G) \leq \frac{1}{p}$. (This bound is attained even for abelian groups, for example in the cyclic group of order p^2.) If G is a p-group of maximal class, then we establish in Theorems 2.10 and 2.11 that $\varrho(G) \leq \frac{p+1}{p^2}$, and we give an example to show that this bound is sharp. We also show at the end of Section 2 that in the case of cube roots, a group G with $\varrho_3(G) > \frac{7}{18}$ is either the direct product of a group of exponent 3 with a cyclic group of order 2 (in which case $\varrho_3(G) = \frac{1}{2}$), or is a 3-group of exponent 9. Section 3 is devoted to square roots. Just as groups with sufficiently many involutions must be elementary abelian 2-groups, it turns out that groups with a non-identity element with sufficiently many square roots must be 2-groups. Theorem 3.11 gives a classification of all finite groups for which $\varrho_2(G) \geq \frac{7}{12}$. In particular, we show that if $\varrho_2(G) > \frac{7}{12}$, then G is a 2-group. This is best possible, because there are infinitely many non 2-groups G for which $\varrho_2(G) = \frac{7}{12}$.

We end this section by recalling some standard notation that we will use throughout the paper.

Notation 1.2. Let G be a finite group. We follow the conventions that $[x, y] = x^{-1}y^{-1}xy$ and that commutators are left-normed, so that for example $[x, y, z]$ means $[[x, y], z]$, for all $x, y, z \in G$. The terms of the lower central series of G are written $\gamma_i(G)$ for $i \geq 2$. That is, $\gamma_2(G) = [G, G] = G'$ and $\gamma_{i+1}(G) = [\gamma_i(G), G]$ for $i > 2$. The terms of the upper central series are denoted $Z_i(G)$ for $i \geq 1$. So $Z_1(G) = Z(G)$, and $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. We will denote by $\Phi(G)$ the Frattini subgroup of G – the intersection of the maximal subgroups of G.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

A p-group of maximal class is a p-group of order p^n for some $n > 1$ which has nilpotency class $n-1$. It is well known that if G is a p-group of maximal class c, then $|Z_i(G)| = p^i$ for $1 \le i \le c-1$ and $|G : \gamma_i(G)| = p^i$ for each $2 \le i \le c$. If G has maximal class, define $G_1 = C_G(\gamma_2(G)/\gamma_4(G))$. That is, G_1 consists of the elements x of G such that $[x, \gamma_2(G)] \le \gamma_4(G)$. This subgroup is sometimes called the fundamental subgroup of G.

A finite p-group G is *regular* if for all $x, y \in G$, there is some $z \in \mho_1(\langle x, y\rangle')$ such that $(xy)^p = x^p y^p z$.

For any finite group G and prime p we define

$$\mathcal{I}(G) = \mathcal{I}_p(G) = \{x \in G : x^p = 1\};$$
$$\alpha(G) = \alpha_p(G) = \tfrac{|\mathcal{I}_p(G)|}{|G|}.$$

If G is a finite p-group we define, for all positive integers i,

$$\Omega_i(G) = \langle x \in G | x^{p^i} = 1\rangle;$$
$$\mho_i(G) = \langle x^{p^i} | x \in G\rangle;$$
$$M(G) = \{a \in G : \ (ax)^p = x^p \text{ for all } x \in G\}.$$

Finally, C_n will denote the cyclic group of order n.

2. **General Results**

We begin by stating some results on p-groups that we will need. Throughout this section we will write $\varrho(G)$ for $\varrho_p(G)$. An excellent introduction to regular p-groups and p-groups of maximal class is given by the lecture notes of Fernandez-Alcober [4]; the standard graduate text in English on p-groups is Berkovich's book [1]. A large number of results on p-groups are also contained in Kapitel III of Huppert [6].

The following theorem is proved in [4]; alternatively it follows from [1, Theorem 9.6].

Lemma 2.1. [1, Theorem 7.1(b)] *Let G be a p-group. If G has nilpotency class less than p, or if $|G| \le p^p$, or if $\exp(G) = p$, then G is regular.*

Proposition 2.2. [1, Theorem 7.2(a)–(d)] *Let G be a regular p-group and i a positive integer. Then*

(a) *For all x, y in G, $x^{p^i} = y^{p^i}$ if and only if $(xy^{-1})^{p^i} = 1$.*
(b) $\Omega_i(G) = \{x \in G : x^{p^i} = 1\}$;
(c) $\mho_i(G) = \{x^{p^i} : x \in G\}$;
(d) $|G| = |\Omega_i(G)| \times |\mho_i(G)|$.

Theorem 2.3. [4, Theorem 4.9(i),(ii)] *Let G be a p-group of maximal class of order p^m, where $m \ge p+2$. Then the following statements hold:*

(a) *G_1 is regular.*
(b) *$\mho_1(G_1) = \gamma_p(G)$ and $\mho_1(\gamma_i(G)) = \gamma_{i+p-1}(G)$ for all $i \ge 2$.*

Recall that a *proper section* of a group G is a quotient of a proper subgroup of G.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

Theorem 2.4. [1, Theorem 7.4(b)-(c)] *Let G be a p-group that is irregular but all of whose proper sections are regular. Then*

(a) $\exp(G') = p$;
(b) $Z(G) = \mho_1(G)$;
(c) $M(G) = G'$.

If G is a p-group of maximal class and order p^{p+1}, then $Z(G)$ has order p and G' has index p^2. Moreover any proper subgroup has order at most p^p, so is regular. Thus we may apply Theorem 2.4 to obtain the following immediate corollary.

Corollary 2.5. *Let G be a p-group of maximal class and order p^{p+1}. Then $Z(G) = \mho_1(G) \cong C_p$, and $G' = M(G)$ has exponent p and index p^2.*

In groups such as $C_p^n \times C_2$, half the elements of the group are p^{th} roots of the unique involution. But this rootiness is really just an artefact of G having many elements of order p. Lemma 2.6 shows that when an element of a group G has more p^{th} roots than the identity, its rootiness $\varrho(G)$ is determined by the rootiness of its Sylow p-subgroups, and G can never be rootier than these groups.

Lemma 2.6. *Suppose G is a finite group, and g is a rooty element of G which has more p^{th} roots than the identity. Then $\varrho(G) \leq \varrho(P)$, for any Sylow p-subgroup P of G. Write $|G| = p^n m$, where $\gcd(m,p) = 1$. If $\varrho(G) = \varrho(P)$, then G has exactly m Sylow p-subgroups.*

Proof. Let g be a rooty element of G that has more p^{th} roots than the identity and let r be a positive integer coprime to p. Then there are integers s, t with $rs + tp = 1$. If x and y are roots of g such that $x^r = y^r$, then

$$x = x^{rs+tp} = (x^r)^s (x^p)^t = (y^r)^s (g)^t = y^{rs+tp} = y.$$

Hence g^r has at least as many roots as g. If the order of g is coprime to p, this implies that the identity element has at least as many roots as g, a contradiction. Hence p divides the order of g. Write $o(g) = p^k u$ for some positive integers k and u. Then g^u again has at least as many roots as g, and is contained in some Sylow p-subgroup P of G. Moreover any p^{th} root of g^u has order p^{k+1}, so is also contained in some Sylow p-subgroup. If the Sylow p-subgroups are $P_1, \ldots, P_\lambda$ for some λ, then $R(g^u) \subseteq P_1 \cup P_2 \cup \cdots \cup P_\lambda$. Since all the P_i are isomorphic, $\varrho(P_i) = \varrho(P)$ for all i. Thus $|R(g^u)| \leq \lambda |P| \varrho(P)$. But $g^u \neq 1$, and so g^u cannot have more roots than g (because g is a rooty element). Therefore, $|R(g^u)| = |R(g)|$. Hence

$$|G|\varrho(G) = |R(g^u)| \leq \lambda |P| \varrho(P).$$

That is, $\varrho(G) \leq \frac{\lambda}{m} \varrho(P)$. If we have equality, then $\lambda = m$. □

Lemma 2.6 shows that if we wish to understand groups G in which $\varrho(G)$ is highest, and in particular higher than $\alpha_p(G)$, it makes sense to restrict our attention to p-groups. We begin with an observation about direct products.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

Lemma 2.7. *Let G and H be p-groups with $\varrho(G) \geq \varrho(H)$. Then $\varrho(G \times H) \leq \varrho(G)$ with equality if and only if $\exp(H) = p$.*

Proof. If $\exp(G) = p$, then $\varrho(G) = 0$, which implies $\varrho(H) = 0$ and thus $\exp(H) = p$. Therefore, $\varrho(G \times H) = 0 = \varrho(G)$, so the result holds. Assume, then, that $\exp(G) > p$. For a in G and b in H we have $|R((a,b))| = |R(a)||R(b)|$. Suppose (a,b) is a rooty element of $G \times H$. Then either $a \neq 1$ or $b \neq 1$, or both, and $|G||H|\varrho(G \times H) = |R((a,b))|$. If $a \neq 1$, then $|R(a)| \leq |G|\varrho(G)$. Thus $\varrho(G \times H) \leq \varrho(G) \times \frac{|R(b)|}{|H|} \leq \varrho(G)$, with equality if and only if $R(b) = |H|$, which is possible precisely when $b = 1$ and H has exponent p. Now suppose $a = 1$. Then $b \neq 1$ and by the same argument $\varrho(G \times H) \leq \varrho(H)$ with equality only when G has exponent p. Since G does not have exponent p, in this case we have $\varrho(G \times H) < \varrho(H) \leq \varrho(G)$. Thus $\varrho(G \times H) \leq \varrho(G)$ with equality if and only if $\exp(H) = p$. □

Lemma 2.7 means that the existence of a group G with a given rootiness ϱ implies that there are infinitely many such groups, obtained by taking the direct product of G with any group H of exponent p. The fact that $\varrho(C_{p^2}) = \frac{1}{p}$ therefore provides infinitely many examples of groups whose rootiness is $\frac{1}{p}$; if p is odd, then in particular we can obtain both abelian and non-abelian examples in this manner.

Lemma 2.8. *Suppose G is an abelian p-group. Then $\varrho(G) \leq \frac{1}{p}$, with equality if and only if $G \cong C_{p^2} \times C_p^k$ for some $k \geq 0$.*

Proof. If G has exponent p, then $\varrho(G) = 0$ and there is nothing to prove. So suppose not. If G is cyclic of order p^n, then $n > 1$ and $\varrho(G) = \frac{1}{p^{n-1}}$, which is at most $\frac{1}{p}$ with equality precisely when $G \cong C_{p^2}$. If G is not cyclic, then $G \cong A \times B$ for some non-trivial A and B and without loss of generality $\varrho(A) \geq \varrho(B)$. Inductively $\varrho(A) \leq \frac{1}{p}$ with equality if and only if $A \cong C_{p^2} \times C_p^i$ for some non-negative i. By Lemma 2.7, $\varrho(G) \leq \varrho(A)$ with equality if and only if $\exp(B) = p$. The result follows immediately. □

Proposition 2.9. *Let G be a regular p-group. Then either $\exp(G) = p$ and $\varrho(G) = 0$, or $\varrho(G) = \frac{1}{|\mho_1(G)|} \leq \frac{1}{p}$. Moreover, $\varrho(G) = \frac{1}{p}$ if and only if G has subgroup A of index p and exponent p, along with a cyclic subgroup H of order p^2, such that $|A \cap H| = p$ and $G = AH$.*

Proof. Assume that $\exp(G) > p$, or there is nothing to prove. Then $\mho_1(G)$ is a nontrivial subgroup of G and, by Proposition 2.2(b), $\Omega_1(G)$ has exponent p. Let X be a transversal of $\Omega_1(G)$. For x in X and a in $\Omega_1(G)$, setting $y = ax$ we have $(xy^{-1})^p = a^{-p} = 1$. Hence $y^p = x^p$ by Proposition 2.2(a). Conversely, if $x, y \in X$ with $x^p = y^p$, then $(xy^{-1})^p = 1$, meaning $xy^{-1} \in \Omega_1(G)$ and so $x = y$. Therefore, the set of roots of x^p is precisely $x\Omega_1(G)$. Hence, by Proposition 2.2(d), $\varrho(G) = \frac{|\Omega_1(G)|}{|G|} = \frac{1}{|\mho_1(G)|} \leq \frac{1}{p}$. We have equality precisely when $|\mho_1(G)| = p$. In this case, write $A = \Omega_1(G)$. Then A has exponent p and index p. For any element x of $G - A$, the subgroup H generated by x has order p^2. Moreover $|A \cap H| = p$ and $G = AH$, as required. Conversely, if G has subgroups A and H as described, then since H contains an element of order p^2 we know $\mho_1(G)$ is nontrivial, but since A has exponent p we know $\Omega_1(G)$ has index at most p. The only possibility is that $|\mho_1(G)| = p$, and thus $\varrho(G) = \frac{1}{p}$. □

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

Theorem 2.10. *Let m be any positive integer with $m \geq p+2$. If G is a p-group of maximal class and order p^m, then $\varrho(G) \leq \frac{1}{p} + \frac{1}{p^{m+1-p}} \leq \frac{1}{p} + \frac{1}{p^3}$.*

Proof. Let m be any positive integer with $m \geq p+2$. Suppose G is a p-group of maximal class and order p^m, and let g be a rooty element of G. By Theorem 2.3, G_1 is regular and $\mho_1(G_1) = \gamma_p(G)$. Therefore, $\varrho(G_1) = \frac{1}{|\gamma_p(G)|}$ by Proposition 2.9. Since G has maximal class, $|\gamma_p(G)| = p^{m-p}$, so that $\varrho(G_1) = \frac{1}{p^{m-p}}$. At most $\frac{1}{p-1}$ of the elements of $G - G_1$ can be roots of g (as if x is a root, then x^2, x^3,...,x^{p-1} are not). Hence

$$\begin{aligned} \varrho(G)|G| = |R(g)| &\leq \tfrac{1}{p-1}|G - G_1| + |G_1|\varrho(G_1) \\ &= \tfrac{p^m - p^{m-1}}{p-1} + \tfrac{p^{m-1}}{p^{m-p}} \\ &= p^{m-1} + p^{p-1} \\ \varrho(G) &\leq \tfrac{1}{p} + \tfrac{1}{p^{m+1-p}} \leq \tfrac{1}{p} + \tfrac{1}{p^3}. \end{aligned}$$

□

Theorem 2.11. *Suppose $|G| = p^{p+1}$. If $\varrho(G) > \frac{1}{p}$, then $\varrho(G) = \frac{p+1}{p^2}$.*

Proof. Suppose $\varrho(G) > \frac{1}{p}$ and let g be a rooty element. Then G must be irregular by Proposition 2.9. Hence G is of maximal class. Then, by Corollary 2.5, $\mho_1(G)$ has order p, meaning $\exp(G) = p^2$. Moreover $M(G)$ has index p^2 and exponent p. If there is an element a of order p lying outside of $M(G)$, then the subgroup $\langle a \rangle M(G)$ also has exponent p, so $R(g) \cup R(g^2) \cup \cdots \cup R(g^{p-1}) \subseteq G - \langle a \rangle M(G)$. Hence $\varrho(G) \leq \frac{1}{p}$. So we can assume all elements outside $M(G)$ have order p^2, meaning precisely $\frac{1}{p-1}$ of them are roots of g. Hence $\varrho(G) = \frac{p+1}{p^2}$. □

The case $\varrho(G) = \frac{p+1}{p^2}$ in Theorem 2.11 does occur, as the following example shows. It is one of two commonly given examples of irregular p-groups of minimal order; the other being the Sylow p-subgroups of the symmetric group on p^2 elements (which can be show to have rootiness $\frac{1}{p}$).

Example 2.12. Let $G = \langle a_1, a_2, \ldots, a_{p-1}, b \rangle$, where $a_1^{p^2} = 1, a_i^p = 1$ for $2 \leq i \leq p-1$, $b^p = a_1^p$ and all generators commute except that $b^{-1}a_i b = a_i a_{i+1}$ when $1 \leq i < p-1$, and $b^{-1}a_{p-1}b = a_{p-1}a_1^{-p}$. That G is of maximal class, irregular, and of order p^{p+1}, is shown in [4, Example 2.4]. It is also shown that $G' = \Omega_1(G) = \langle a_1^p, a_2, \ldots, a_{p-1} \rangle$ in this group. Therefore, G' has exponent p and no element outside of G' can have order p. As in the proof of Theorem 2.11, we now have $\varrho(G) = \frac{p+1}{p^2}$.

We end this section with a couple of results limiting, for odd primes, the possible kinds of non p-groups with high values of ϱ_p. We first state a result due to Laffey.

Theorem 2.13. [7, Laffey] *Let p be an odd prime. If G is not a p-group, then $\alpha_p(G) \leq \frac{p}{p+1}$.*

Theorem 2.14. *Let p be an odd prime. Suppose $\varrho_p(G) > \frac{p}{2(p+1)}$. Then either G is a p-group, or $G \cong H \times C_2$, where H is a p-group, and $\varrho_p(G) = \frac{1}{2}\alpha_p(H)$.*

Proof. Let g be a rooty element, and write $\lambda = |R(g)|$, so that $\lambda > \frac{p}{2(p+1)}|G|$. Now g^r also has λ p^{th} roots, whenever r is coprime to p. If $m > p$, then g, g^2 and g^{p+1} each have λ roots. If $p > m \geq 3$, then g, g^2 and g^3 each have λ roots. But $3\lambda > |G|$, a contradiction. Therefore, either $m = 2$ or $m = p$. For any root x of g, both x and x^2 lie in the centralizer of g. Hence, $|C_G(g)| \geq \frac{p}{p+1}|G| > \frac{1}{2}|G|$. Therefore, g is central in G. Now consider $\overline{G} = G/\langle g\rangle$. If $m = 2$, then the 2λ elements of G that are roots of elements of $\langle g\rangle$ map onto λ elements of $G/\langle g\rangle$ that have order dividing p. Hence $\alpha_p(\overline{G}) > \frac{p|G|}{2(p+1)|\overline{G}|} = \frac{p}{p+1}$. Theorem 2.13 now implies that $\overline{G}$ is a p-group. Hence $|G| = 2p^n$ for some n. This means G has a unique Sylow p-subgroup H, which is therefore normal. Hence $G = H\langle g\rangle \cong H \times C_2$, and clearly $\varrho_p(G) = \frac{1}{2}\alpha_p(H)$. The remaining possibility is that $o(g) = p$. In this case, each of $g, g^2,\ldots,g^{p-1}$ has λ p^{th} roots. So in $\overline{G}$, they become $\frac{p-1}{p}\lambda$ elements of order p. Hence (not forgetting that the identity element of $\overline{G}$ also has order dividing p), we get

$$\alpha_p(\overline{G}) > \frac{p-1}{p} \cdot \frac{p}{2(p+1)} \cdot \frac{|G|}{|\overline{G}|} = \frac{p(p-1)}{2(p+1)} \geq \frac{p}{p+1}.$$

Hence $\overline{G}$ is a p-group, which implies that G is also a p-group. □

We remark that there do exist 'non-trivial' instances of non p-groups with high rootiness – that is, groups with elements having more p^{th} roots than the identity. For example there is a group G of order 36 with $\varrho_3(G) = \frac{1}{3}$ but $\alpha_3(G) = \frac{1}{12}$. We can improve slightly on Theorem 2.14 for the case $p = 3$, thanks to another result of Laffey.

Theorem 2.15. [8, Laffey] *Let G be a finite group. If $\alpha_3(G) \geq \frac{7}{9}$, then G is a 3-group and either $\alpha_3(G) = \frac{7}{9}$ or G has exponent 3.*

This allows us to show that the only non-trivial examples of groups with cube rootiness greater than $\frac{7}{18}$ occur in 3-groups.

Theorem 2.16. *Suppose G is a finite group with $\varrho_3(G) \geq \frac{7}{18}$. Then either*

(a) *$G \cong H \times C_2$, where H is a group of exponent 3, and $\varrho(H) = \frac{1}{2}$;*
(b) *$G \cong H \times C_2$, where H is a 3-group with $\alpha_3(H) = \frac{7}{9}$, and $\varrho(H) = \frac{7}{18}$; or*
(c) *G is a 3-group of exponent 9 and nilpotency class at most 4.*

Proof. Suppose G is a finite group with $\varrho(G) \geq \frac{7}{18}$. Suppose first that G is not a 3-group. By Theorem 2.14 then, $G \cong H \times C_2$, where H is a 3-group with $\varrho_3(G) = \frac{1}{2}\alpha_3(H)$. By assumption $\varrho_3(G) \geq \frac{7}{18}$. Hence by Theorem 2.15, either $\alpha_3(G) = \frac{7}{9}$ or G has exponent 3. This deals with parts (a) and (b). It remains to deal with the case that G is a 3-group. Suppose this is the case, and let g be a rooty element, with R the set of cube roots of g. Now g^{-1} and g^2, which as G is a 3-group are both distinct from g, also have $|R|$ cube roots. Therefore, $g^{-1} = g^2$ and $o(g) = 3$. More than $\frac{7}{9}$ of the elements of G cube to an element of $\langle g\rangle$, because every element of $R \cup R^{-1} \cup \langle g\rangle$ has this property. Hence g is central; write as usual, $\overline{G}$ for $G/\langle g\rangle$. We have $\alpha_3(\overline{G}) > \frac{7}{9}$, which implies, by Theorem 2.15, that $\overline{G}$ has exponent 3. Consequently every element of G cubes to an element of $\langle g\rangle$, meaning G has exponent 9. Clearly G must have class at least 3, or else G would be regular and its rootiness would be most $\frac{1}{3}$. It is well-known that a group of exponent 3 has class at most 3. Thus $\overline{G}$ has class at most 3, forcing G to have class at most 4. □

We note that there are groups G with $\varrho_3(G) > \frac{7}{18}$. Example 2.12 provides an irregular 3-group G of order 81 with $\varrho(G) = \frac{4}{9}$. It can also be shown that there is a 3-group K of order 3^7 such that $\varrho_3(K) = \frac{13}{27}$ so, at least for $p = 3$, it is possible for $\varrho_p(G) > \frac{p+1}{p^2}$. As we shall see in the next section, this is very different from the case $p = 2$.

3. Square Roots

In this section we investigate groups with many nontrivial square roots. Just as groups with sufficiently many involutions must be elementary abelian 2-groups, it turns out that groups with a non-identity element with sufficiently many square roots must be 2-groups. As an indication of what happens, the database of small groups in Magma's free online calculator [10], or in GAP [5], can be interrogated easily to find all 2-groups G of order at most 64 such that $\varrho_2(G) > \frac{1}{2}$. The outcome is summarised in Observation 3.2. In all cases, if $\varrho_2(G) > \frac{7}{12}$, then $\varrho_2(G) \in \{\frac{5}{8}, \frac{3}{4}\}$. Theorem 3.11 will show that this holds for all finite groups G, by classifying all finite groups for which $\varrho_2(G) \geq \frac{7}{12}$. In particular, we show that if $\varrho_2(G) > \frac{7}{12}$, then G is a 2-group. Before we proceed, we need to establish some notation that will be used in this section.

Notation 3.1. We denote by C_n the cyclic group of order n; D_{2n} is the dihedral group of order $2n$, and Q_{4n} is the generalised quaternion group of order $4n$ given by

$$Q_{4n} = \langle a, b : a^{2n} = 1, b^2 = a^n, ba = a^{-1}b \rangle.$$

We write D_8^{*r} for the central product of r copies of D_8 (with the convention that D_8^{*0} is the trivial group). Note that D_8^{*r} is one of the extraspecial 2-groups of order 2^{2r+1}, for $r \geq 1$: the other is $D_8^{*(r-1)} * Q_8$. For each positive integer r we define a group

$$W_r = \langle c, x_1, y_1, \ldots, x_r, y_r \rangle,$$

where $c^2 = x_i^2 = y_i^2 = 1$ and all pairs of generators commute except $[c, x_i] = y_i$, for all i. Finally, we will encounter a certain group of order 32 for which it will be useful to have a name:

$$\mathcal{M}_{32} := \langle a, b, c : a^4 = b^4 = c^4 = 1, ba = ab, ca = a^{-1}c, cb = b^{-1}c, c^2 = a^2 \rangle.$$

During this section, we will write $\alpha_2(G)$ and $\varrho_2(G)$ (as defined in Section 1) in the formal statements of results, for easy cross-referencing, but will usually write $\alpha(G)$ and $\varrho(G)$ elsewhere. Similarly, we will write $\mathcal{I}(G)$ for $\mathcal{I}_2(G)$, the set of elements x of G for which $x^2 = 1$.

Observation 3.2. There are eighteen 2-groups G of order at most 64 with $\varrho_2(G) > \frac{1}{2}$. Of these, four have $\varrho_2(G) = \frac{3}{4}$. These are precisely the groups $Q_8 \times E$, where E is trivial or an elementary abelian 2-group. A further seven groups have $\varrho_2(G) = \frac{5}{8}$. These are precisely the groups $Q_{16} \times E$, or

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

$(D_8 * Q_8) \times E$, or $\mathcal{M}_{32} \times E$, where E is trivial or elementary abelian, and $\mathcal{M}_{32}$ is the group of order 32 defined in Notation 3.1. The remaining seven of the eighteen groups have $\frac{1}{2} < \varrho_2(G) \leq \frac{9}{16}$.

We note that there are infinitely many groups G with $\varrho_2(G) > \frac{1}{2}$, because Q_{8n}, where n is any even positive integer, has square rootiness $\frac{1}{2} + \frac{1}{4n}$. There are also infinitely many 2-groups with this property. For example the extraspecial group $D_8^{*r} * Q_8$ of order 2^{2r+3} has square rootiness $\frac{1}{2} + \frac{1}{2^{r+2}}$ (see Proposition 3.5).

We first state Wall's classification of groups with many involutions.

Theorem 3.3. [11, Wall] *Suppose H is a finite group for which $\alpha(H) > \frac{1}{2}$. Then H is either an elementary abelian 2-group, or the direct product of an elementary abelian 2-group with a group H_0 of one of the following types.*

(I) H_0 is generalised dihedral. Specifically, H_0 has an abelian subgroup A_0 of index 2 which does not admit a cyclic group of order 2 as a direct factor, and H_0 is generated by A_0 along with an involution c with the property that $cac^{-1} = a^{-1}$ for all $a \in A_0$;
(II) $H_0 \cong D_8 \times D_8$;
(III) $H_0 \cong D_8^{*r}$, some $r \geq 1$;
(IV) $H_0 \cong W_r$, some $r \geq 1$.

Lemma 3.4. *Suppose $\varrho_2(G) > \frac{1}{2}$, with g a rooty element. Then g is a central involution, G is non-abelian, and $Z(G)$ is an elementary abelian 2-group. Moreover*

(a) *If $Z(G) \not\leq \Phi(G)$, then $G \cong G_0 \times E$, where E is an elementary abelian 2-group, $\varrho_2(G_0) = \varrho_2(G)$ and $Z(G_0) \leq \Phi(G_0)$.*
(b) *For any $h \in Z(G) - \langle g \rangle$, $\varrho_2(G/\langle h \rangle) = \varrho_2(G)$.*

Proof. Both g^{-1} and any conjugate of g have the same number of roots as g. Therefore, $g = g^{-1}$ and g is central. Suppose $a \in Z(G)$. Then for any root x of g we have $(xa)^2 = ga^2$. Thus, to avoid a contradiction, it must be that $ga^2 = g$. Hence $a^2 = 1$ and $Z(G)$ is an elementary abelian 2-group. Clearly now G cannot be abelian, else $Z(G)$ would equal G and g would have no square roots at all.

(a) Suppose $Z(G)$ is not contained in $\Phi(G)$. Let a be an element of $Z(G) - \Phi(G)$. Then there is a maximal subgroup U of G which does not contain a. Moreover since a is central, a is an involution that centralises, but is not contained in, U. Hence $G \cong U \times \langle a \rangle$, and clearly $\varrho_2(G) = \varrho_2(U)$. Note too that $\Phi(G) \cong \Phi(U)$. Repeating this step for any further elements of $Z(G) - \Phi(G)$ we obtain the required decomposition of G.
(b) For any $h \in Z(G) - \langle g \rangle$, and any x in G, we have that $(xh)^2 = x^2$. That is, x is a root if and only if xh is a root. Hence $\varrho_2(G/\langle h \rangle) = \varrho_2(G)$, as required. □

The next result obtains $\alpha_2(G)$ and $\varrho_2(G)$ in the case where G is an extraspecial 2-group.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

Proposition 3.5. *Let $r \geq 1$.*

$$\alpha_2(D_8^{*r}) = \frac{2^r+1}{2^{r+1}} \qquad \varrho_2(D_8^{*r}) = \frac{2^r-1}{2^{r+1}}$$

$$\alpha_2(D_8^{*(r-1)} * Q_8) = \frac{2^r-1}{2^{r+1}} \qquad \varrho_2(D_8^{*(r-1)} * Q_8) = \frac{2^r+1}{2^{r+1}}.$$

Proof. Note that for any extraspecial 2-group G, we have $\mho_1(G) = Z(G) \cong C_2$. Therefore, if g is the unique central involution, every element is either contained in $\mathcal{I}(G)$ or in $R(g)$. Thus $\alpha(G)+\varrho(G) = 1$. Therefore, it is sufficient in each case to verify the expression for $\alpha(G)$. We proceed by induction, the result being easy to check for $r = 1$ (where the groups involved are D_8 and Q_8), so suppose $r > 1$. Write D for $D_8^{*(r-1)}$. The elements of $D * D_8$ are of the form xy where $x \in D$ and $y \in \{1, a, b, c\}$, with $a^2 = 1$, $b^2 = 1$ and $c^2 = g$, where g is the central involution of D. Now $(xy)^2 = x^2y^2$, so $(xy)^2 = 1$ when $x^2 = y^2$, and $(xy)^2 = g$ otherwise. Hence

$$\alpha(D * D_8) = \tfrac{|D|}{|D*D_8|}\left(3\alpha(D) + \varrho(D)\right) = \frac{1}{4}\left(\frac{3(2^{r-1}+1)}{2^r} + \frac{2^{r-1}-1}{2^r}\right) = \frac{2^r+1}{2^{r+1}}.$$

For $D * Q_8$ we follow the same procedure, except that in this case elements of G are of the form xy where $x \in D$ and $y \in \{1, u, v, w\}$ where $u^2 = v^2 = w^2 = g$. The recurrence relation this time is $\alpha(D * Q_8) = \frac{1}{4}(\alpha(D) + 3\varrho(D))$, and a quick check shows that this results in $\alpha(D * Q_8) = \frac{2^r-1}{2^{r+1}}$. □

Proposition 3.6. *Suppose $\alpha(H) > \frac{7}{12}$. Then either H is an elementary abelian 2-group, with $\alpha(H) = 1$, or H is the direct product of an elementary abelian 2-group with a group H_0, where $\alpha(H) = \alpha(H_0)$ and H_0 is one of the following groups (listed in decreasing order of $\alpha(H_0)$).*

- $\alpha(H) = \frac{3}{4}$ *and* $H_0 \cong D_8$;
- $\alpha(H) = \frac{2}{3}$ *and* $H_0 \cong D_6$;
- $\alpha(H) = \frac{5}{8}$ *and H_0 is one of D_{16}, $D_8 * D_8$, W_2, or the generalised dihedral group whose abelian index 2 subgroup is $C_4 \times C_4$;*
- $\alpha(H) = \frac{3}{5}$ *and* $H_0 \cong D_{10}$.

Proof. Assume H is not elementary abelian. Since $\alpha(H) > \frac{1}{2}$, we have that H is one of the groups described in Theorem 3.3, so that H is the direct product of an elementary abelian 2-group with an H_0 of one of the given four types. Observe that $\alpha(H) = \alpha(H_0)$.

First, let H_0 be of type I. That is, H_0 is generalised dihedral, the semidirect product of a non-trivial abelian group A_0 with a group $\langle c\rangle$, where c is an involution which inverts every element of A_0. Moreover A_0 does not have C_2 as a direct factor. Write $A_0 = \mathcal{O} \times \mathcal{T}$, where $\mathcal{O}$ is a subgroup of odd order ω and $\mathcal{T}$ is an abelian 2-group (or the trivial group). Then $|\mathcal{I}(H_0)| = \frac{1}{2}|H_0| + |\mathcal{I}(\mathcal{T})|$. Hence $\alpha(H) = \alpha(H_0) = \frac{1}{2} + \frac{1}{2\omega}\alpha(\mathcal{T})$. By assumption, none of the components of $\mathcal{T}$ is cyclic of order 2. If $\mathcal{T} \cong \{1\}$, then $\alpha(\mathcal{T}) = 1$. If $\mathcal{T} \cong C_4$, then $\alpha(\mathcal{T}) = \frac{1}{2}$; for all other $\mathcal{T}$ we have $\alpha(\mathcal{T}) \leq \frac{1}{4}$. So, if $\omega \geq 7$, then $\alpha(H) \leq \frac{1}{2} + \frac{1}{14} < \frac{7}{12}$. If $\omega = 5$, then either $A_0 \cong C_5$ and $\alpha(H) = \frac{3}{5}$, or $\alpha(H) \leq \frac{1}{2} + \frac{1}{20} < \frac{7}{12}$. If $\omega = 3$, then either $A_0 \cong C_3$ and $\alpha(H) = \frac{2}{3}$, or $\alpha(H) \leq \frac{1}{2} + \frac{1}{12} = \frac{7}{12}$. If $\omega = 1$, then $A_0 \cong C_4$ results in $\alpha(H) = \frac{3}{4}$; $A \cong C_8$ or $A_0 \cong C_4 \times C_4$ give $\alpha(H) = \frac{5}{8}$; all other possibilities give $\alpha(H) \leq \frac{9}{16}$. In

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

summary, if $\alpha(H) = \frac{3}{4}$, then $H_0 \cong D_8$. If $\alpha(H) = \frac{2}{3}$, then $H_0 \cong D_6$. If $\alpha(H) = \frac{3}{5}$, then $H_0 \cong D_{10}$. If $\alpha(H) = \frac{5}{8}$, then $H_0 \cong D_{16}$ or H_0 is the generalised dihedral group whose abelian index 2 subgroup is $C_4 \times C_4$. In all other cases, $\alpha(H) \leq \frac{7}{12}$.

For types II and III, if $H_0 \cong D_8 \times D_8$, then it is easy to check that $\alpha(H_0) = \frac{9}{16} < \frac{7}{12}$. If H_0 is extraspecial, then by Proposition 3.5, $\alpha(H) > \frac{7}{12}$ if and only if either $H_0 \cong D_8$, with $\alpha(H) = \frac{3}{4}$, or $H_0 \cong D_8 * D_8$, with $\alpha(H) = \frac{5}{8}$. The final type to consider is when $H_0 \cong W_r$. Let $A_0 = \langle x_1, \ldots, x_r, y_1, \ldots, y_r\rangle$. Certainly $A_0 \subseteq \mathcal{I}(H_0)$, so consider $x \in H_0 - A_0$. Then $x = c\prod_{i=1}^{r}(x_i^{a_i} y_i^{b_i})$ where each a_i and each b_i is either zero or one. Because conjugation by c sends x_i to $x_i y_i$, and fixes y_i, we have $x^2 = \prod_{i=1}^{r} y_i^{a_i}$. Hence $x^2 = 1$ if and only if $a_i = 0$ for all i, which implies that $\mathcal{I}(H_0) = |A_0| + 2^r$. Since $|H_0| = 2^{2r+1}$, we obtain $\alpha(H) = \frac{1}{2} + \frac{1}{2^{r+1}}$. The only instances where $\alpha(H) > \frac{7}{12}$ are when $r = 1$ (which gives D_8 again) or when $r = 2$, which gives W_2, with $\alpha(W_2) = \frac{5}{8}$. □

Theorem 3.7. *If $\varrho_2(G) > \frac{1}{2}$, g is a rooty element and $G/\langle g\rangle$ is elementary abelian, then $G \cong D_8^{*r} * Q_8$ or $G \cong (D_8^{*r} * Q_8) \times E$, where E is an elementary abelian 2-group and r is a non-negative integer. Moreover, $\varrho_2(G) = \frac{2^{r+1}+1}{2^{r+2}}$.*

Proof. Notice that g is a central involution of G, by Lemma 3.4. Hence $\langle g\rangle$ is normal in G, so $G/\langle g\rangle$ is well-defined. Moreover $|G| = 2|G/\langle g\rangle|$, which means in particular that G is a 2-group. Consequently, $\Phi(G)$ is contained in every normal subgroup with an elementary abelian quotient. Thus $\Phi(G) \leq \langle g\rangle$. Obviously $\Phi(G)$ cannot be trivial; hence $\Phi(G) = \langle g\rangle$. By Lemma 3.4 (a), we may reduce to the case where $Z(G) \leq \Phi(G)$. The fact that G is a non-abelian 2-group now forces $Z(G) = G' = \Phi(G)$. Hence G is extraspecial. The result now follows immediately from Proposition 3.5. □

Corollary 3.8. *If $\varrho_2(G) \geq \frac{3}{4}$, then $\varrho_2(G) = \frac{3}{4}$ and G is either Q_8 or the direct product of Q_8 with an elementary abelian 2-group.*

Proof. Suppose $\varrho_2(G) \geq \frac{3}{4}$ with g a rooty element. The proportion of elements of G whose square is either 1 or g is just $\varrho_2(G) + \alpha(G)$. Now g is a central involution, meaning that $(xg)^2 = x^2$ for any $x \in G$. Hence $\alpha(G/\langle g\rangle) = \varrho_2(G) + \alpha(G) > \varrho_2(G) \geq \frac{3}{4}$. Using Proposition 3.6, we see that $G/\langle g\rangle$ is an elementary abelian 2-group. Now we employ Theorem 3.7. The only case in that theorem which gives $\varrho_2(G) \geq \frac{3}{4}$ is when $r = 0$, meaning that $\varrho_2(G) = \frac{3}{4}$ and G is either Q_8 or the direct product of Q_8 with an elementary abelian 2-group. □

Theorem 3.9. *Suppose $\varrho_2(G) > \frac{1}{2}$, and let g be a rooty element of G. Suppose $G/\langle g\rangle \cong D_{2q} \times E$, for some odd prime q and some elementary abelian 2-group E. Then $\varrho_2(G) \leq \frac{2q+1}{4q}$, with equality if and only if G is isomorphic to either Q_{8q} or the direct product of Q_{8q} with an elementary abelian 2-group.*

Proof. Write $\overline{G} = G/\langle g\rangle$, and for x in G write $\overline{x}$ for the corresponding element of $\overline{G}$. Let x be an element of order q in G, and write $N = \langle x\rangle$. Then $\overline{N\langle g\rangle}$ is the unique Sylow q-subgroup of $\overline{G}$. Since $\overline{x}^{\overline{G}} = \{\overline{x}, \overline{x}^{-1}\}$, we see that $x^G \subseteq \{x, x^{-1}, xg, (xg)^{-1}\}$. But xg and xg^{-1} have order $2q$, so cannot be conjugate to x. Moreover x cannot be central in G because $Z(G)$ is an elementary abelian 2-group

(Lemma 3.4). Hence $x^G = \{x, x^{-1}\}$, which means $C_G(x)$ has index 2 in G, and is therefore normal. Let K be a Sylow 2-subgroup of $C_G(x)$; it has index q in $C_G(x)$. Both K and N normalise K, which means (since $C_G(x) = \langle K, N\rangle$) that K is normal in $C_G(x)$, and so K is the unique Sylow 2-subgroup of $C_G(x)$; hence it is characteristic in $C_G(x)$ and consequently normal in G. Therefore, K is contained in, and has index 2 in, every Sylow 2-subgroup of G. There must be more than one Sylow 2-subgroup of G, because every root of g is contained in a Sylow 2-subgroup. Hence there are q Sylow 2-subgroups; call them $P_1, \dots, P_q$. Note that, when $i \neq j$, we have $P_i \cap P_j = K$. By Corollary 3.8, we have that $\rho_2(P_1) \leq \frac{3}{4}$. Hence $|R \cap P_1| \leq \frac{3}{4}|P_1|$. Therefore,

$$R \subseteq P_1 \cdot \cup (P_2 - K) \cdots \dot\cup (P_q - K)$$

$$|R| \leq \tfrac{3}{4}|P_1| + \sum_{i=2}^{q} |P_i - K|$$

$$|R| \leq \tfrac{3}{4}|P_1| + (q-1)\tfrac{|P_1|}{2}$$

$$\varrho_2(G) \leq \tfrac{3}{4q} + \tfrac{q-1}{2q} = \tfrac{2q+1}{4q}$$

with equality precisely when $\varrho_2(P_1) = \frac{3}{4}$ and K is a subgroup of index 2 in P_1 such that every element of $P_1 - K$ has order 4. By Corollary 3.8 we have that $P_1 \cong Q_8 \times C_2^k$ for some $k \geq 0$, and the only suitable K is (isomorphic to) $C_4 \times C_2^k$. Recalling that x centralises K, we have that $G = NP_1 \cong NQ_8 \times C_2^k \cong Q_{8q} \times C_2^k$. For example, if u is any element of order 4 in K, and b is any element of order 4 in $P_1 - K$, then setting $a = ux$ we have $\langle a, b\rangle \cong Q_{8q}$ and $G \cong \langle a, b\rangle \times C_2^k$. □

Lemma 3.10. *If $\alpha(H) > \frac{1}{2}$, then $Z(H)$ is an elementary abelian 2-group.*

Proof. Since $\alpha(H) > \frac{1}{2}$, we have, by Theorem 3.3, that H is either an elementary abelian 2-group, or the direct product of an elementary abelian 2-group with a group H_0 of one of four given types. It is therefore sufficient to show that $Z(H_0)$ is an elementary abelian 2-group for all possible H_0. If H_0 is generalised dihedral and A_0 is the abelian subgroup of index 2, then conjugation by any involution outside A_0 inverts every element of A_0. Hence the central elements are precisely the involutions of A_0 (plus the identity), and we are done. If H_0 is $D_8 \times D_8$, then $Z(H_0)$ is $C_2 \times C_2$. If H_0 is extraspecial, then $Z(H_0)$ is cyclic of order 2. Finally if H_0 is W_r, then c conjugates x_i to $x_i y_i$ and commutes with y_i, for all i. Thus $Z(H_0) = \langle y_1, \dots, y_r\rangle$. Therefore, in all cases, $Z(H)$ is an elementary abelian 2-group. □

We may now complete the classification of groups with square rootiness at least $\frac{7}{12}$. Recall that $\mathcal{M}_{32}$ is the group of order 32 whose presentation was given in Notation 3.1.

Theorem 3.11. *Suppose $\varrho_2(G) \geq \frac{7}{12}$. Then G is isomorphic to G_0, or the direct product of G_0 with an elementary abelian 2-group, where G_0 is one of the following groups.*

(a) $G_0 \cong Q_8$ *and* $\varrho_2(G) = \frac{3}{4}$;
(b) $G_0 \cong Q_{16}$ *and* $\varrho_2(G) = \frac{5}{8}$;

(c) $G_0 \cong D_8 * Q_8$ *and* $\varrho_2(G) = \frac{5}{8}$*;*
(d) $G_0 \cong \mathcal{M}_{32}$ *and* $\varrho_2(G) = \frac{5}{8}$*;*
(e) $G_0 \cong Q_{24}$ *and* $\varrho_2(G) = \frac{7}{12}$*.*

For the purposes of the proof, we write B for the generalised dihedral group of order 32 whose abelian subgroup of index 2 is $C_4 \times C_4$. This is one of the groups given in Proposition 3.6.

Proof. Let g be a rooty element of G, and as usual write $\overline{G} = G/\langle g\rangle$. The fact that $\varrho(G) \geq \frac{7}{12}$ implies that $\alpha(\overline{G}) > \frac{7}{12}$, so $\overline{G}$ is one of the groups H listed in Proposition 3.6. If H_0 is D_6 or D_{10}, then by Theorem 3.9 the only possibility for which $\varrho(G) \geq \frac{7}{12}$ is when G is Q_{24} (or its direct product with an elementary abelian 2-group), and here $\varrho(G) = \frac{7}{12}$. All the other possible H given by Proposition 3.6 are 2-groups. Hence if G is not a 2-group, the theorem holds.

We assume from now on that G is a 2-group, and proceed by induction on $|G|$. For the base case, if $|G| \leq 64$, then the result holds by Observation 3.2. If H is an elementary abelian 2-group, then by Theorem 3.7 $\varrho(G) = \frac{2^r+1}{2^{r+1}}$ for some positive integer r. Since $\varrho(G) \geq \frac{7}{12}$ the only possibilities are $r = 1$ and $r = 2$. These result in the cases $G_0 \cong Q_8$ and $G_0 \cong D_8 * Q_8$ above. If $\varrho(G) \geq \frac{3}{4}$, then by Corollary 3.8, we have the case $G_0 \cong Q_8$. We may therefore assume that $\frac{7}{12} < \varrho < \frac{3}{4}$, and that H_0 is either D_8, $D_8 * D_8$, D_{16}, B or W_2. In the first case $\alpha(H_0) = \frac{3}{4}$; in the last four cases $\alpha(H_0) = \frac{5}{8}$.

Suppose $\alpha(H_0) = \frac{5}{8}$. If $Z(G) \neq \langle g\rangle$, then G has a central involution h with $h \neq g$, and $\varrho(G/\langle h\rangle) = \varrho(G)$, which by assumption lies strictly between $\frac{7}{12}$ and $\frac{3}{4}$. By induction $\varrho(G) = \frac{5}{8}$. But since $\alpha(H_0) = \frac{5}{8}$, at most $\frac{5}{8}$ of the elements of G square to 1 or g. Since G contains at least one involution, we have $\varrho(G) < \frac{5}{8}$, a contradiction. Therefore, if $\alpha(H_0) = \frac{5}{8}$, then $Z(G) = \langle g\rangle$.

Return now to the general case where $\alpha(H_0) \in \{\frac{3}{4}, \frac{5}{8}\}$. Let K be the subgroup of G such that $\overline{K} = Z\left(G/\langle g\rangle\right)$. We will analyse the elements of $K - Z(G)$. Let $a \in K - Z(G)$. Then $a^x \in a\langle g\rangle$ for all $x \in G$. Thus, since a is non-central, $C_G(a)$ has index 2 in G. Write $X = G - C_G(a)$. For any $x \in X$ we have $(ax)^2 = a(xax^{-1})x^2 = a^2x^2g$. Lemma 3.10 tells us that $\overline{K}$ is an elementary abelian 2-group. Therefore, $a^2 \in \{1, g\}$, meaning either a is an involution, or a is a root of g.

Assume first, for a contradiction, that a is an involution. Then $(ax)^2 = x^2g$. Thus x is a root if and only if $ax \in \mathcal{I}(G)$. Hence at most half the elements of X are roots. That is, $|R \cap X| \leq \frac{1}{4}|G|$. This forces

$$|R \cap C_G(a)| \geq |R| - \tfrac{1}{4}|G| \geq \tfrac{7}{12}|G| - \tfrac{1}{4}|G| = \tfrac{1}{3}|G| = \tfrac{2}{3}|C_G(a)|.$$

Inductively, this forces $C_G(a)$ to be Q_8 or its direct product with an elementary abelian 2-group. Therefore, $\varrho(C_G(a)) = \frac{3}{4}$ and every element of $C_G(a)$ must square to 1 or g.

Now $\alpha(\overline{G}) > \varrho(G)$, so $\alpha(\overline{G}) > \frac{7}{12}$. We see from Proposition 3.6 that either $\overline{G}$ is elementary abelian, or $\alpha(\overline{G}) \leq \frac{3}{4}$. The case where $\overline{G}$ is elementary abelian has been dealt with in Corollary 3.8, so we can assume $\alpha(\overline{G}) \leq \frac{3}{4}$. That means at least a quarter of the elements h of G have the property that $h^2 \notin \{1, g\}$. Such elements, then, cannot be contained in $C_G(a)$. Therefore, X contains at least $\frac{1}{4}|G|$ elements h such that $h^2 \notin \{1, g\}$. The remaining elements of X consist of pairs $\{x, ax\}$ exactly one of which is a root (the other being an involution). So at most a quarter of the elements of X are roots.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

But now

$$|R| = |R \cap X| + |R \cap C_G(a)| \le \tfrac{1}{4}|X| + \tfrac{3}{4}|C_G(a)| = \tfrac{1}{2}|G|,$$

a contradiction.

Hence every element of $K - Z(G)$ is a root. Let us consider the case where $H_0 \cong D_8 * D_8$ in a little more detail. We have shown above that, since $\alpha(H_0) = \frac{5}{8}$, we have $Z(G) = \langle g \rangle$. As H_0 is extraspecial, $|K| = 4$. Let a be either of the two elements of $K - Z(G)$. Then $\overline{a}$ is the non-identity element of $Z(\overline{G})$. Elements of G which do not square to 1 or g must then square to a or ag. Thus, $\frac{5}{8}$ of the elements of G square to 1 or g, and $\frac{3}{8}$ of the elements of g square to a or ag. If $x^2 = a$, then x commutes with a and so $x \in C_G(a)$. Also a is conjugate to ag (because a isn't central) via some element w of G and so if $x^2 = a$, then $(x^w)^2 = ag$. Now $C_G(a)$ is a normal subgroup of a and thus contains x^w. Therefore, $C_G(a)$ contains all of the $\frac{3}{8}|G|$ roots of a and ag. The remaining $\frac{1}{8}|G|$ elements of $C_G(a)$ are either roots or square to the identity. Now for any root $b \in C_G(a)$, we have $(ab)^2 = 1$; and vice versa, if $z \in \mathcal{I}(C_G(a))$, then $(az)^2 = g$. That is $|R \cap C_G(a)| = |\mathcal{I}(C_G(a))|$. Hence $C_G(a)$ contains precisely $\frac{1}{16}|G|$ involutions and the same number of roots. So even if every element of $G - C_G(a)$ is a root, $\varrho(G) \le \frac{9}{16} < \frac{7}{12}$, a contradiction. Therefore, H_0 must be one of D_8, D_{16}, B, or W_2, and we have noted that if $\alpha(H_0) = \frac{5}{8}$, then $Z(G) = \langle g \rangle$. By Lemma 3.4(a), we may further assume that $Z(G) \le \Phi(G)$. We will show that under these assumptions, $|G| \le 64$.

Since every element of $K - Z(G)$ is a root, we see from Corollary 3.8 that $|K : Z(G)| \le 4$. Now

$$|G : K| = |\overline{G} : \overline{K}| = |\overline{G} : Z(\overline{G})| = |H_0 : Z(H_0)|.$$

Thus

$$|G| = |G : K||K : Z(G)||Z(G)| \le 4|H_0 : Z(H_0)||Z(G)|.$$

If H_0 is any of W_2, D_{16} or B, then $|H_0 : Z(H_0)| = 8$. Combining this with the fact that $|Z(G)| = 2$ gives $|G| \le 64$.

We are left with the case $H_0 = D_8$. Here $|H_0 : Z(H_0)| = 4$, so $|G| \le 16|Z(G)|$. Recall that $Z(G) \le \Phi(G)$. In particular, $\langle g \rangle \le \Phi(G)$, which means that $\langle g \rangle$ is contained in every maximal subgroup V of G. Therefore, $\overline{V}$ is maximal in $\overline{G}$ if and only if V is maximal in G. Hence $\overline{\Phi(G)} = \Phi(\overline{G}) \cong \Phi(H_0) \cong C_2$. Therefore, $|Z(G)| \le |\Phi(G)| = 2|\Phi(\overline{G})| = 4$. Hence, again, $|G| \le 64$. By Observation 3.2, G is one of the groups listed in the statement of Theorem 3.11, and the proof is complete. □

We note that the classification of all finite groups with $\varrho_2(G) > \frac{1}{2}$ is one of the aims of the second author's thesis, which is in preparation.

References

[1] Y. Berkovich, *Groups of prime power order*, Vol. 1, Walter de Gruyter, Berlin (2008).

[2] Y. Berkovich, On the number of solutions of the equation $x^{p^k} = a$ in a finite p-group, *Proc. American Math. Soc.*, **116** (1992) 585–590.

[3] N. Blackburn, Note on a paper of Berkovich, *J. Algebra*, **24** (1973) 323–334.

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582

[4] G. A. Fernández-Alcober, An introduction to finite p-groups: regular p-groups and groups of maximal class, *Mat. Contemp.*, **20** (2001) 155–226.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.10.2; 2019. https://www.gap-system.org.

[6] B. Huppert, *Endliche Gruppen I*, Grundlehren der Mathematischen Wissenschaften, **134**, Springer-Verlag, Berlin, (1967).

[7] T. J. Laffey, The Number of Solutions of $x^p = 1$ in a Finite Group, *Mathematical Proceedings of the Cambridge Philosophical Society*, **80** (1976) 229–31.

[8] T. J. Laffey, The Number of Solutions of $x^3 = 1$ in a 3-group, *Math. Zeitschrift.*, **149** (1976) 43–45.

[9] T. Y. Lam, On the number of solutions of $x^{p^k} = a$ in a p-group, *Illinois J. Math.*, **32** (1988) 575–583.

[10] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993), *J. Symbolic Comput.*, **24** (1997) 235–265.

[11] C. T. C. Wall, On groups consisting mostly of involutions, *Proc. Camb. Phil. Soc.*, **67** (1970) 251–262.

Sarah B. Hart

Department of Economics, Mathematics and Statistics, Birkbeck College, University of London, Malet Street, London WC1E 7HX, UK

Email: s.hart@bbk.ac.uk

Daniel McVeagh

Department of Economics, Mathematics and Statistics, Birkbeck College, University of London, Malet Street, London WC1E 7HX, UK

Email: d.mcveagh@bbk.ac.uk

DOI: http://dx.doi.org/10.22108/ijgt.2020.119870.1582