ON THE NUMBER OF PRIME ORDER SUBGROUPS OF FINITE GROUPS

TIMOTHY C. BURNESS and STUART D. SCOTT

(July 3, 2009)

Abstract

Let G be a finite group and let $\delta(G)$ be the number of prime order subgroups of G. We determine the groups G with the property $\delta(G) > |G|/2-1$, extending earlier work of C. T. C. Wall, and we use our classification to obtain new results on the generation of near-rings by units of prime order.

Keywords and phrases: Finite groups; Prime order subgroups; Near-rings
AMS Mathematics subject classification: 20D06, 20D10, 16Y30.

1. Introduction

Let G be a finite group and let $\delta(G)$ be the number of prime order subgroups of G. In this paper we determine the groups G with $\delta(G) > |G|/2-1$. As our main theorem demonstrates (see Theorem 1 below), such a group has a rather simple structure which is easy to describe. In particular, we find that A_5 is the only nonsoluble group with this property, while $\delta(G) = |G|/2$ if and only if $G = Z_2$ or $S_3 \times D_8 \times E$ with $\exp(E) \leq 2$ (where $\exp(E)$ denotes the exponent of E).

One of our main motivations comes from a theorem of C. T. C. Wall. In [18], Wall classifies the finite groups G with the property $i_2(G) > |G|/2-1$, where $i_2(G)$ is the number of involutions in G. Since $\delta(G) \geq i_2(G)$, our main theorem is a natural extension of Wall's result.

Related problems have been investigated by various authors. For example, Liebeck and MacHale [7] classify the finite groups in which more than half of the elements are inverted by some automorphism of the group, extending earlier work of Manning and Miller (see [8] and [9], for example). All such groups are soluble, and the aforementioned theorem of Wall follows as a corollary. In fact, Potter [13] has proved that the proportion of elements in a nonsoluble group which are inverted by an automorphism is at most $4/15$. For soluble groups, recent work of Hegarty [4] attempts to bound this proportion in terms of the derived length of the group.

In order to state our main theorem, we first need to define a collection of groups. We say that a nontrivial finite group G belongs to the collection $\mathcal{L}$ if and only if G is one of the following (up to isomorphism). Here E denotes an elementary abelian 2-group of order 2^n (for some $n \geq 0$) and D_8 is the dihedral group of order 8. We also remind the reader that a *generalized dihedral group* is a group of the form $D(A) = A\langle\tau\rangle = A.2$, where A is abelian and τ acts by inversion.

(I) $G = D(A)$ is a generalized dihedral group, where A is abelian;

(II) $G = D_8 \times D_8 \times E$;

(III) $G = H(r) \times E$, where $H(r) \cong (D_8 \times \cdots \times D_8)/Z_2^{r-1}$ is a central product of $r \geq 1$ copies of D_8 so that

$$H(r) = \langle x_1, y_1, \ldots, x_r, y_r, z \mid \; x_i^2 = y_i^2 = z^2 = 1, \text{ all pairs of generators commute except } [x_i, y_i] = z\rangle;$$

(IV) $G = S(r) \times E$, where $S(r)$ is the split extension of an elementary abelian group of order 2^{2r} ($r \geq 1$) by a cyclic group $Z_2 = \langle z\rangle$ so that

$$S(r) = \langle x_1, y_1, \ldots, x_r, y_r, z \mid \; x_i^2 = y_i^2 = z^2 = 1, \text{ all pairs of generators commute except } [z, x_i] = x_i y_i\rangle;$$

(V) $G = T(r)$ is the split extension of an elementary abelian group A of order 2^{2r} ($r \geq 1$) by a cyclic group $Z_3 = \langle z\rangle$ so that

$$T(r) = \langle x_1, y_1, \ldots, x_r, y_r, z \mid \; x_i^2 = y_i^2 = z^3 = 1, \text{ all pairs of generators commute except } [z, x_i] = x_i y_i \text{ and } [z, y_i] = x_i\rangle;$$

(VI) G is a group of exponent 3;

(VII) $G = S_3 \times D_8 \times E$;

(VIII) $G = S_3 \times S_3$;

(IX) $G = S_4$;

(X) $G = A_5$.

In this list, groups of type (I)–(IV) correspond respectively to the groups labelled I–IV by Wall (see [18, pp. 261–262]); these are precisely the finite groups G with the property $i_2(G) > |G|/2 - 1$. A group of type (VI) is nilpotent of class at most three and we refer the reader to [17, Theorem 5.2.1] for additional information on such groups. We also note that $D(Z_3) \cong S_3$, $D(Z_4) = D_8$, $T(1) \cong A_4$ and $D(A) \times E \cong D(A \times E)$, while $D(E) \cong E \times Z_2$ is an elementary abelian 2-group.

It is not difficult to see that the only overlap between the classes (I)–(X) are groups of the form $D_8 \times E$ with $\exp(E) \leq 2$, which appear in (I) (with $A = Z_4 \times E$), (III) and (IV) (both with $r = 1$). We can now state our main theorem.

THEOREM 1. *Let G be a nontrivial finite group and let $\delta(G)$ be the number of prime order subgroups of G. Then $\delta(G) > |G|/2 - 1$ if and only if $G \in \mathcal{L}$. The precise value of $\delta(G)$ for each $G \in \mathcal{L}$ is listed in Table 1.*

	Type of G	$\lvert G\rvert$	$\delta(G)$
(I)	$D(A)$	$2\lvert A\rvert$	$\lvert G\rvert/2+\delta(A)$
(II)	$D_8 \times D_8 \times E$	2^{n+6}	$9\lvert G\rvert/16-1$
(III)	$H(r) \times E$	2^{2r+n+1}	$\lvert G\rvert/2+2^{n+r}-1$
(IV)	$S(r) \times E$	2^{2r+n+1}	$\lvert G\rvert/2+2^{n+r}-1$
(V)	$T(r)$	3.2^{2r}	$2\lvert G\rvert/3-1$
(VI)	Exponent 3	3^m	$(\lvert G\rvert-1)/2$
(VII)	$S_3 \times D_8 \times E$	3.2^{n+4}	$\lvert G\rvert/2$
(VIII)	$S_3 \times S_3$	36	19
(IX)	S_4	24	13
(X)	A_5	60	31

TABLE 1. Values of $\delta(G)$, $G \in \mathcal{L}$

COROLLARY 1. *Let G be a finite group. Then $\delta(G) \geq 3|G|/4$ if and only if G is an elementary abelian 2-group.*

REMARK 1. In view of Corollary 2.5 below, we deduce that $\delta(G) \geq 3|G|/4$ if and only if $i_2(G) \geq 3|G|/4$.

COROLLARY 2. *Let G be a finite group with* $\exp(G) \geq 3$. *Then $\delta(G) > 2|G|/3$ if and only if $G = D(A)$ and either $A = Z_4 \times E$ with* $\exp(E) = 2$, *or* $\exp(A) = 3$.

The next corollary follows immediately from Theorem 1.

COROLLARY 3. *Let G be a finite group. Then $\delta(G) = |G|/2$ if and only if $G = Z_2$ or $S_3 \times D_8 \times E$ with* $\exp(E) \leq 2$.

In the final section of this paper we describe an application of Theorem 1 to the study of *near-rings*. Recall that a near-ring is a set R with two binary operations $+$ and $\cdot$ such that $(R,+)$ is a group (not necessarily abelian) and $\cdot$ satisfies a single distributive law. For example, if G is a finite group then the set of functions from G to G which fix the identity element has the structure of a near-ring with respect to the operations $(f+g)(x) = f(x)g(x)$ and $(f \cdot g)(x) = f(g(x))$, where $x \in G$. We write $M_0(G)$ to denote this particular near-ring associated to G.

There are several results in the literature concerning the generation of $M_0(G)$ by units (that is, bijections) of prescribed order. For example, in [15] it is shown that $M_0(G)$ is generated by a unit of order two if and only if $\exp(G) \geq 3$ and $G \neq Z_3$. Similarly, the $M_0(G)$ which can be generated by a unit of order 3 are determined in [16]. Bounds on the proportion of units of arbitrary order which generate $M_0(G)$

are established in [10]; upper and lower bounds are given as functions of $|G|$ and $i_2(G)$. Roughly speaking, the proportion is high if and only if $i_2(G)/|G|$ is small.

The main theorem of [14] states that if p is a prime number then either $M_0(G)$ is generated by a unit of order p, or G is an elementary abelian 2-group with $|G| \not\equiv 1 \bmod p$, or G belongs to a finite collection of groups. Moreover, this finite collection can be defined in terms of δ and p, and we can use Theorem 1 to obtain various results on the exceptional groups which arise. We refer the reader to Section 6 for more details.

This paper is organised as follows. In Section 2 we record a number of useful results which we will need in the proof of Theorem 1. Some of these results are new and may be of independent interest. In particular, Lemma 2.16 provides a sharp upper bound for the number of elements of order three in a finite nonsoluble group. Next, in Section 3, we prove that $G = A_5$ is the only nonabelian simple group with $\delta(G) > |G|/2-1$; we extend this result to all nonsoluble groups in the following section. In Section 5 we assume G is soluble and we complete the proof of Theorem 1 by establishing the nonexistence of a minimal counterexample. It is worth noting that our proof uses the main theorem of [18]. Here we also establish Corollaries 1 and 2, and justify the precise values of $\delta(G)$ listed in Table 1. The aforementioned application to near-rings is discussed in Section 6.

Notation. Our group theoretic notation is standard. If G and H are groups then $G.H$ denotes an unspecified extension of G by H, while $\exp(G)$ is the exponent of G. If m is a positive integer then G^m denotes the direct product of m copies of G. We use Z_n to denote the cyclic group of order n and write D_n for the dihedral group of order n. We adopt the notation of [5] for groups of Lie type. In particular, we write $\mathrm{L}_n(q) = \mathrm{L}_n^+(q) = \mathrm{PSL}_n(q)$, $\mathrm{U}_n(q) = \mathrm{L}_n^-(q) = \mathrm{PSU}_n(q)$, $E_6^+(q) = E_6(q)$ and $E_6^-(q) = {}^2E_6(q)$. If X is a subset of a finite group G and r is a positive integer then $i_r(X)$ denotes the number of elements of order r in X. We sometimes write $|g|$ for the order of a group element g, while $\lfloor x \rfloor$ denotes the largest integer less than or equal to the real number x.

Acknowledgements. The first author would like to thank the Department of Mathematics at the University of Auckland for its generous hospitality while this paper was in preparation. We also thank Bob Guralnick for some interesting comments, and we thank both referees for their careful reading and helpful remarks.

2. Preliminaries

Let G be a finite group and let $\delta(G)$ be the number of prime order subgroups of G. If r is a positive integer and X is a subset of G then let $i_r(X)$ be the number of elements of order r in X. Then

$$\delta(G) = \sum_{r \in \pi(G)} (r-1)^{-1} i_r(G), \tag{1}$$

where $\pi(G)$ is the set of distinct prime divisors of $|G|$.

LEMMA 2.1. *Let G be a finite group and let N be a normal subgroup of G. Then*

$$\delta(G) \leq \delta(N) + |N| \cdot \delta(G/N).$$

Proof. It suffices to show that $i_p(G) \leq i_p(N) + |N| \cdot i_p(G/N)$ for any prime p which divides $|G|$. Suppose $x \in G$ has order p, so either $x \in N$ or $Nx \in G/N$ has order p. The desired bound follows since there are precisely $i_p(G/N)$ elements of order p in G/N, and $i_p(Ny) \leq |N|$ for all $y \in G \setminus N$. □

COROLLARY 2.2. *Let G be a finite group with a normal subgroup N such that $\delta(G/N) \leq |G/N|/2 - 1$. Then $\delta(G) \leq |G|/2 - 1$.*

Proof. This follows immediately from Lemma 2.1 since $\delta(N) \leq |N| - 1$. □

LEMMA 2.3. *Let G be a finite group such that $3 + 3i_2(G) + i_3(G) \leq |G|$. Then $\delta(G) \leq |G|/2 - 1$.*

Proof. As in (1) we have

$$\begin{aligned}\delta(G) = \sum_{r \in \pi(G)} (r-1)^{-1} i_r(G) = i_2(G) + \frac{1}{2} i_3(G) + \sum_{r \geq 5} (r-1)^{-1} i_r(G) \\ \leq i_2(G) + \frac{1}{2} i_3(G) + \frac{1}{4}(|G| - i_2(G) - i_3(G) - 1) \\ = \frac{1}{4}|G| + \frac{1}{4}(3 + 3i_2(G) + i_3(G)) - 1\end{aligned}$$

and the result follows. □

In view of Lemma 2.3, it will be useful to have upper bounds on the number of elements of order two and three in various finite groups.

LEMMA 2.4. *Let G be a finite group with an automorphism α such that $S = \{x \in G : \alpha(x) = x^{-1}\}$ has more than $3|G|/4$ elements. Then G is abelian and $S = G$.*

Proof. This is [18, Lemma 7]. □

COROLLARY 2.5. *Let G be a finite group. Then $i_2(G) \geq 3|G|/4$ if and only if G is an elementary abelian 2-group.*

Proof. Take α to be the identity automorphism in Lemma 2.4. □

COROLLARY 2.6. *Let G be a finite group, let N be a nonabelian normal subgroup of G, and let $x \in G \setminus N$ be an involution. Then $i_2(Nx) \leq 3|N|/4$.*

Proof. Let $\alpha \in \mathrm{Aut}(N)$ be the automorphism induced by conjugation by x. Then $nx \in Nx$ is an involution if and only if $\alpha(n) = n^{-1}$, so Lemma 2.4 implies that $i_2(Nx) \leq 3|N|/4$ since N is nonabelian. □

LEMMA 2.7. *Let G be a finite group with an abelian subgroup N. Then $i_2(Nx)$ divides $|N|$ for any involution $x \in G \setminus N$.*

Proof. Let H be the set of elements $n \in N$ such that nx is an involution. Then H is a subgroup of N since N is abelian, so the result follows from Lagrange's Theorem. □

LEMMA 2.8. *Let G be a finite group with a subgroup N of odd order. Then $i_2(Nx)$ divides $|N|$ for any involution $x \in G \setminus N$.*

Proof. This follows from [3, Lemma 4.1(i), §10.4]. Indeed, we have $i_2(Nx) = |N : C_N(x)|$. □

LEMMA 2.9. *Let G be a finite nonsoluble group. Then $i_2(G) \leq 4|G|/15 - 1$.*

Proof. This follows from the main theorem of [13]. □

LEMMA 2.10. *Let G be a finite group with a normal subgroup N. If $x \in G \setminus N$ has order r then $i_r(Nx) = i_r(Ny)$ for all cosets Ny which are G/N-conjugate to Nx.*

Proof. Suppose Ny is G/N-conjugate to Nx, so $Ny = Nz^{-1}xz$ for some $z \in G$. Then the map $\varphi : Nx \to Ny$, defined by $nx \mapsto z^{-1}nxz$, induces a bijection between the subset of elements of order r in Nx and the corresponding subset of Ny. □

LEMMA 2.11. *Let G be a finite group with a normal subgroup N, where N is an elementary abelian p-group. Then the following hold:*

(i) If $x \in G \setminus N$ has order 2 then $i_2(Nx) = |N|$ if and only if x inverts N elementwise, that is $x^{-1}nx = n^{-1}$ for all $n \in N$.

(ii) If $x \in C_G(N) \setminus N$ has prime order $r \neq p$ then $i_r(Nx) = 1$.

(iii) If $x \in G \setminus N$ has prime order r then $i_r(Nx) = p^d$ for some integer d. In particular, if $i_r(Nx) < |N|$ then $i_r(Nx) \leq |N|/p$.

Proof. Parts (i) and (ii) are trivial, so let us consider (iii). Suppose N has order p^m. We can view N as an m-dimensional vector space over $\mathbb{F}_p$, so $\mathrm{Aut}(N) \cong \mathrm{GL}_m(p)$. Now conjugation by x induces an automorphism of N, so we can identify x with an invertible $\mathbb{F}_p$-linear map $A : N \to N$ of order r.

Now $nx \in Nx$ has order r if and only if $n(I + A + \cdots + A^{r-1}) = 0$, where I denotes the identity linear map $N \to N$. If $r \neq p$ then basic linear algebra implies that this condition holds if and only if $n \in \mathrm{im}(I - A)$, so $i_r(Nx) = p^{m-\alpha}$ where $\alpha = \dim C_N(A)$. Similarly, if $r = p$ then the condition $n \in \ker(I + A + \cdots + A^{r-1})$ implies that $i_r(Nx) = p^{m-\beta}$, where β is the number of indecomposable blocks of size p in the Jordan form of A on N. □

LEMMA 2.12. *Let G be a finite group with an index-two subgroup N such that $i_2(G \setminus N) > |G|/3$. Then $N = N_1 \times N_2$, where $N_1 \leq Z(N)$ has odd order and N_2 is a 2-group.*

Proof. Let $a \in G \setminus N$ be an involution and let $\Lambda = \{n_i a : 1 \leq i \leq m\}$ be a set of distinct involutions in the coset Na, where $m > |G|/3 = 2|N|/3$. Fix $j \in \{1, \ldots, m\}$ and define $\Lambda_j = \{n_i n_j a : 1 \leq i \leq m\}$. Note that $|\Lambda \cap \Lambda_j| > |N|/3$. Let $x \in \Lambda \cap \Lambda_j$, so $x = n_k n_j a$ for some $k \in \{1, \ldots, m\}$. Since $x \in \Lambda$ we have $x^2 = 1$ and we quickly deduce that $n_k \in C_N(n_j)$. Therefore, $|C_N(n_j)| \geq |\Lambda \cap \Lambda_j| > |N|/3$ and thus $C_N(n_j)$ has index at most 2 in N. In particular, $C_N(n_j)$ is normal in N and it contains every element of odd order in N. Moreover, if $y \in N$ has odd order then $n_j \in C_N(y)$ for all $1 \leq j \leq m$, hence $y \in Z(N)$ since $m > 2|N|/3$. Therefore, the set of elements of odd order in N forms a central subgroup, N_1 say, and it follows that $N = N_1 \times N_2$, where N_2 is a 2-group (possibly trivial). □

The next lemma provides rather accurate bounds on $i_2(G)$, $i_3(G)$ and $|G|$ in the case where G is a simple group of Lie type. In view of the isomorphisms $G_2(2)' \cong \mathrm{U}_3(3)$ and ${}^2G_2(3)' \cong \mathrm{L}_2(8)$, in Table 2 we regard $G_2(2)'$ and ${}^2G_2(3)'$ as classical groups. In addition, we regard the Tits group ${}^2F_4(2)'$ as a sporadic group and it is therefore omitted from Table 2.

LEMMA 2.13. *Let G be a finite simple group of Lie type over $\mathbb{F}_q$. For $r \in \{2,3\}$ we have*

$$i_r(G) \leq i_r(\mathrm{Aut}(G)) < 2(1+q^{-1})q^{f(G,r)},$$

where the values of $f(G,r)$ are recorded in Table 2. In the table we also record a lower bound $|G| > g(G)$.

Proof. The upper bounds on $i_r(\mathrm{Aut}(G))$ are given in [6, Proposition 1.3]. If G is classical then the lower bound on $|G|$ follows from [1, Proposition 3.9], while the corresponding bound for exceptional groups can be checked directly (using [6, Lemma 1.2], for example). □

To close this preliminary section we will establish an analogue of Lemma 2.9 for elements of order 3. First we require the following technical result.

LEMMA 2.14. *Let G be a nonabelian finite simple group. Then the following hold:*

(i) If $G \neq \mathrm{L}_2(8)$ then $1 + i_3(\mathrm{Aut}(G)) \leq 7|G|/20$;

(ii) If $G = \mathrm{L}_2(8)$ then $1 + i_3(\mathrm{Aut}(G)) = 225|G|/504$;

(iii) $|\mathrm{Out}(G)|^2 \leq |G|/15$.

In parts (i) and (iii), equality holds if and only if $G = A_5$.

G	$f(G,2)$	$f(G,3)$	$g(G)$
$\mathrm{L}_n^{\pm}(q)$	$(n^2+n-2)/2$	$(2n^2+n-3)/3$	$\frac{1}{2}(q+1)^{-1}q^{n^2-1}$
$\mathrm{PSp}_n(q)'$	$(n^2+2n)/4$	$(2n^2+3n)/6$	$\frac{1}{4}q^{(n^2+n)/2}$
$\mathrm{P}\Omega_n^{\pm}(q)$	$n^2/4$	$(2n^2-n)/6$	$\frac{1}{8}q^{(n^2-n)/2}$
$\Omega_n(q)$	$(n^2-1)/4$	$(2n^2-n-1)/6$	$\frac{1}{4}q^{(n^2-n)/2}$
$E_8(q)$	128	168	$\frac{1}{2}q^{248}$
$E_7(q)$	70	91	$\frac{1}{4}q^{133}$
$E_6^{\pm}(q)$	42	54	$\frac{1}{6}q^{78}$
$F_4(q)$	28	36	$\frac{1}{2}q^{52}$
$G_2(q)$	8	10	$\frac{1}{2}q^{14}$
${}^3D_4(q)$	16	20	$\frac{1}{2}q^{28}$
${}^2F_4(q)$	14	18	$\frac{1}{2}q^{26}$
${}^2G_2(q)$	4	5	$\frac{1}{2}q^{7}$
${}^2B_2(q)$	3	11/3	$\frac{1}{2}q^{5}$

TABLE 2. Bounds on $i_2(G), i_3(G)$ and $|G|$

Proof. First consider (i). If G is a sporadic group then $i_3(\mathrm{Aut}(G)) = i_3(G)$ and the character table of G is available in the GAP Character Table Library [2]. The desired result quickly follows.

Next suppose $G = A_n$, where $n \geq 5$. Again, we have $i_3(\mathrm{Aut}(G)) = i_3(G)$ since $|\mathrm{Out}(G)|$ is not divisible by 3. Now, if $G = A_5$ then $i_3(G) = 20$ and thus $1+i_3(\mathrm{Aut}(G)) = 7|G|/20$ in this case. Now assume $n \geq 6$. Then

$$i_3(G) = \sum_{k=1}^{\lfloor n/3 \rfloor} \frac{n!}{k!(n-3k)!3^k} \leq \left(\frac{1}{3(n-3)!} + \frac{1}{18} \sum_{k=2}^{\lfloor n/3 \rfloor} \frac{1}{(n-3k)!} \right) n!$$

and we have

$$\sum_{k=2}^{\lfloor n/3 \rfloor} \frac{1}{(n-3k)!} < \sum_{l=0}^{\infty} \frac{1}{(3l)!} < \sum_{l=0}^{\infty} \frac{1}{6^l} = \frac{6}{5}. \tag{2}$$

Therefore, for $n \geq 6$ we get

$$1+i_3(\mathrm{Aut}(G)) \leq 1 + \frac{1}{18}\left(1+\frac{6}{5}\right) n! < \frac{7}{20}|G|$$

as required.

Finally, let us assume G is a group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is prime. First suppose $G = \mathrm{L}_2(q)$. Note that we may assume $q \geq 7$ since $\mathrm{L}_2(2)$ and $\mathrm{L}_2(3)$ are not simple, while $\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5$. Now $i_3(G) \leq |\mathrm{GL}_2(q)|/(q-1)^2 = q(q+1)$ and any element $x \in \mathrm{Aut}(G) \setminus G$ of order 3 is a field automorphism. Therefore

$$\begin{aligned} 1+i_3(\mathrm{Aut}(G)) &\leq 1+q(q+1)+2\alpha\left(\frac{|\mathrm{PGL}_2(q)|}{|\mathrm{PGL}_2(q^{1/3})|}\right) \\ &= 1+q(q+1)+2\alpha \cdot q^{2/3}(q^{4/3}+q^{2/3}+1), \end{aligned}$$

where $\alpha = 1$ if $\log_p q$ is divisible by 3, otherwise $\alpha = 0$. Since $|G| = (2,q-1)^{-1}q(q^2-1)$, where $(2,q-1)$ denotes the highest common factor of 2 and $q-1$, it is easy to check that $1+i_3(\mathrm{Aut}(G)) < 7|G|/20$ for all $q \geq 7$ with $q \neq 8$. However, if $G = \mathrm{L}_2(8)$ then $1+i_3(\mathrm{Aut}(G)) = 225$ and (ii) follows.

Now assume $G \neq \mathrm{L}_2(q)$. Here we apply the bound on $i_3(\mathrm{Aut}(G))$ given in Lemma 2.13. For example, suppose $G = \mathrm{L}_n^{\pm}(q)$, where $n \geq 3$. In view of Lemma 2.13, it suffices to show that

$$1+2(1+q^{-1})q^{f(G,3)} \leq \frac{7}{20}g(G),$$

where the terms $f(G,3)$ and $g(G)$ are given in Table 2. The reader can check that this bound holds unless $(n,q) = (4,2)$, or $n = 3$ and $q \leq 13$. These small cases can be checked directly. The remaining groups of Lie type are handled in a similar fashion and we leave the details to the reader. (Note that we may assume $q \geq 3$ if $G = G_2(q)'$ since $G_2(2)' \cong \mathrm{U}_3(3)$. Similarly, we may assume $q \geq 27$ if $G = {}^2G_2(q)$, and $q \geq 8$ if $G = {}^2B_2(q)$.)

Now let us consider part (ii). If $|\mathrm{Out}(G)| \leq 2$ then $|\mathrm{Out}(G)|^2 \leq |G|/15$, with equality if and only if $G = A_5$. Therefore we may assume $|\mathrm{Out}(G)| > 2$. If $G = A_6$ then $|\mathrm{Out}(G)|^2 = 16 < |G|/15$, so we can assume G is a group of Lie type. Suppose $G = \mathrm{L}_2(q)$, where $q \geq 7$. Then $|\mathrm{Out}(G)| = (2,q-1)\log_p q$ and it is easy to check that

$$((2,q-1)\log_p q)^2 < (2,q-1)^{-1}q(q^2-1)/15$$

for all $q \geq 7$. Next suppose $G = \mathrm{L}_n^{\pm}(q)$, where $n \geq 3$. Here $|\mathrm{Out}(G)| = 2(n,q\mp 1)\log_p q$, so in view of Lemma 2.13 it suffices to show that

$$4(q+1)^2(\log_p q)^2 < \frac{1}{15}g(G),$$

where $g(G)$ is defined in Table 2. One can verify that this bound holds unless $n = 3$ and $q \leq 3$; these cases can be checked directly. The other cases are entirely similar and we omit the details (see [5, p. 170] for a convenient list of the orders $|\mathrm{Out}(G)|$). □

REMARK 2.15. We note that if $G = \mathrm{L}_2(8)$ then $1+i_3(G) = 57 < 7|G|/20$.

LEMMA 2.16. *Let G be a nonsoluble finite group. Then* $i_3(G) \leq 7|G|/20 - 1$.

Proof. We proceed by induction on $|G|$. Seeking a contradiction, suppose

$$i_3(G) > \frac{7}{20}|G| - 1. \tag{3}$$

Let L be the soluble radical of G. Now

$$i_3(G)+1 \leq |L|\cdot i_3(G/L)+i_3(L)+1 \leq |L|\cdot(i_3(G/L)+1)$$

and thus $i_3(G/L) > 7|G/L|/20 - 1$. In particular, if L is nontrivial then the inductive hypothesis implies that G/L is soluble, hence G is soluble, a contradiction. Therefore, we may assume L is trivial.

Now let N be a minimal normal subgroup of G. Since L is trivial, it follows that N is nonsoluble, so $N \cong J \times \cdots \times J$ is a direct product of isomorphic nonabelian simple groups, with t factors say. By Lemma 2.14(i) (and Remark 2.15), we have

$$i_3(N) = (1+i_3(J))^t - 1 \leq \left(\frac{7}{20}|J|\right)^t - 1 \leq \frac{7}{20}|N| - 1,$$

so (3) implies that there exists $g \in G \setminus N$ of order 3 such that $i_3(Ng) > 7|N|/20$.

If $g \in C_G(N)$ then again Lemma 2.14(i) and Remark 2.15 imply that

$$i_3(Ng) = i_3(N) + 1 \leq \left(\frac{7}{20}|J|\right)^t \leq \frac{7}{20}|N|,$$

with equality if and only if $N = A_5$. Therefore, we may assume that conjugation by g induces a nontrivial automorphism of N, say $\psi_g \in \mathrm{Aut}(N)$.

Now $i_3(Ng) \leq i_3(\mathrm{Inn}(N)\psi_g)$, where $\mathrm{Inn}(N)\psi_g$ is a coset of $\mathrm{Inn}(N) \cong N$ in $\mathrm{Aut}(N) = \mathrm{Aut}(J) \wr S_t$. Suppose $\psi_g \in \mathrm{Aut}(J)^t$. If $J \neq \mathrm{L}_2(8)$ then Lemma 2.14(i) yields

$$i_3(Ng) \leq i_3(\mathrm{Aut}(J)^t) = (1+i_3(\mathrm{Aut}(J)))^t - 1 < \left(\frac{7}{20}|J|\right)^t \leq \frac{7}{20}|N|.$$

Similarly, if $J = \mathrm{L}_2(8)$ then applying Lemma 2.14(ii) we get

$$i_3(Ng) < \left(\frac{225}{504}|J|\right)^t \leq \frac{7}{20}|N|$$

for all $t \geq 2$, while if $t = 1$ we have

$$i_3(Ng) \leq 84 < \frac{7}{20}|N|$$

since any coset of J in $\mathrm{Aut}(J)$ contains at most 84 elements of order 3 (equality if the coset contains field automorphisms).

Now suppose $\psi_g \in \mathrm{Aut}(N) \setminus \mathrm{Aut}(J)^t$, so $t \geq 3$ and $\psi_g = (g_1, \ldots, g_t; \sigma)$, where $g_i \in \mathrm{Aut}(J)$ and $\sigma \in S_t$ has cycle-shape $(3^k, 1^{t-3k})$ for some $k \geq 1$. Then by Lemma 2.14 we have

$$\begin{aligned}
i_3(Ng) \leq i_3(\mathrm{Aut}(J)^t\sigma) &= |\mathrm{Aut}(J)|^{2k}\left(i_3(\mathrm{Aut}(J)^{t-3k}) + 1\right) \\
&\leq \left(\frac{1}{15}|J|^3\right)^k \left((i_3(\mathrm{Aut}(J)) + 1)^{t-3k} - 1 + 1\right) \\
&\leq \left(\frac{1}{15}|J|^3\right)^k \left(\frac{225}{504}|J|\right)^{t-3k} \\
&< \frac{7}{20}|N|.
\end{aligned}$$

We conclude that $i_3(Ng) \leq 7|N|/20$ for all elements $g \in G \setminus N$ of order 3. This final contradiction completes the proof of the lemma. □

REMARK 2.17. It is easy to see that the above argument implies that if G is nonsoluble then $i_3(G) = 7|G|/20 - 1$ if and only if $G = A_5 \times B$ with $i_3(B) = |B| - 1$.

3. Simple groups

In this section we prove

PROPOSITION 3.1. *Let G be a finite simple group. Then one of the following holds:*

(i) $G = Z_2$ *and* $\delta(G) = 1$*;*

(ii) $G = Z_3$ *and* $\delta(G) = 1$*;*

(iii) $G = A_5$ *and* $\delta(G) = 31$*;*

(iv) $\delta(G) \leq |G|/2 - 1$.

If G is an abelian simple group then $G = Z_p$ for some prime p, so $\delta(G) = 1$ and thus Z_2 and Z_3 are the only examples with $\delta(G) > |G|/2 - 1$. Now suppose G is a nonabelian finite simple group. We partition the analysis into a number of separate lemmas, according to the type of G.

LEMMA 3.2. *Let G be a sporadic simple group. Then* $\delta(G) \leq |G|/2 - 1$.

Proof. The character table of G is available in the GAP Character Table Library [2] and it is straightforward to calculate $\delta(G)$ precisely. □

LEMMA 3.3. *Suppose* $G = A_n$ *with* $n \geq 5$. *Then either* $\delta(G) \leq |G|/2 - 1$, *or* $n = 5$ *and* $\delta(G) = 31$.

Proof. The case $n = 5$ can be checked directly, so let us assume $n \geq 6$. In view of Lemma 2.3, it suffices to show that

$$3 + 3i_2(G) + i_3(G) \leq |G|. \tag{4}$$

We have

$$i_2(G) = \sum_{l=1}^{\lfloor n/4 \rfloor} \frac{n!}{(2l)!(n-4l)!2^{2l}} \leq \left(\frac{1}{8(n-4)!} + \frac{1}{4!2^4} \sum_{l=2}^{\lfloor n/4 \rfloor} \frac{1}{(n-4l)!} \right) n!$$

and

$$i_3(G) = \sum_{k=1}^{\lfloor n/3 \rfloor} \frac{n!}{k!(n-3k)!3^k} \leq \left(\frac{1}{3(n-3)!} + \frac{1}{18} \sum_{k=2}^{\lfloor n/3 \rfloor} \frac{1}{(n-3k)!} \right) n!.$$

Now

$$\sum_{l=2}^{\lfloor n/4 \rfloor} \frac{1}{(n-4l)!} < \sum_{l=0}^{\infty} \frac{1}{(4l)!} < \sum_{l=0}^{\infty} \frac{1}{24^l} = \frac{24}{23}$$

and thus (2) implies that

$$3i_2(G) + i_3(G) < \left(\frac{3}{8(n-4)!} + \frac{1}{3(n-3)!} + \frac{3}{4!2^4} \cdot \frac{24}{23} + \frac{1}{18} \cdot \frac{6}{5} \right) n!.$$

We conclude that (4) holds for all $n \geq 6$. □

LEMMA 3.4. *Let $G = \mathrm{L}_2(q)$, where $q \geq 7$. Then $\delta(G) \leq |G|/2 - 1$.*

Proof. As before, it suffices to show that (4) holds. If q is even then

$$i_2(G) = q^2 - 1,\ i_3(G) \leq \frac{|\mathrm{GL}_2(q)|}{(q-1)^2} = q(q+1),\ |G| = q(q^2-1)$$

and thus (4) holds for all $q \geq 8$. Similarly, if q is odd then

$$i_2(G) \leq \frac{|\mathrm{GL}_2(q)|}{2(q-1)^2} = \frac{1}{2}q(q+1),\ i_3(G) \leq q(q+1),\ |G| = \frac{1}{2}q(q^2-1)$$

and again (4) follows. □

LEMMA 3.5. *Suppose $G = \mathrm{L}_4^{\pm}(2)$ or $\mathrm{L}_3^{\pm}(q)$, where $3 \leq q \leq 7$. Then $\delta(G) \leq |G|/2 - 1$.*

Proof. Direct calculation, using GAP [2] for example. □

To deal with the remaining simple groups of Lie type we apply the bounds in Lemma 2.13. Indeed, one can check that if $G \neq \mathrm{L}_2(q)$ is a group of Lie type over $\mathbb{F}_q$, and G is not one of the cases listed in Lemma 3.5, then

$$3 + 3 \cdot 2(1+q^{-1})q^{f(G,2)} + 2(1+q^{-1})q^{f(G,3)} \leq g(G)$$

where the terms $f(G,2)$, $f(G,3)$ and $g(G)$ are given in Table 2. Therefore (4) holds and we are done.

REMARK 3.6. It is interesting to consider the asymptotic behaviour of $\delta(G)$, especially in the case where G is a simple group. Here we expect that $\delta(G)/|G| \to 0$ as $|G| \to \infty$; for example, explicit calculation suggests that $\delta(A_n)/|A_n| < 1/n$ for all $n \geq 8$. This is clearly not true for nonsoluble groups in general. For instance, if $G = A_5 \times E$, where E is elementary abelian of order 2^n, then

$$\delta(G)/|G| = \frac{4}{15} + 2^{-n-2}.$$

Let $p(G)$ be the proportion of *elements* of prime order in a finite group G. It would also be interesting to study the asymptotic behaviour of $p(G)$ when G is a simple group. We note that if G is a group of Lie type of bounded rank then perhaps $p(G)$ does not tend to zero. For example, if q is a *Germain prime*, that is a prime of the form $2p+1$ with p prime, then $i_p(\mathrm{PSL}_2(q)) \approx |G|/2$. However, it is not known whether or not there are infinitely many such primes. The same applies for primes of the form $cp+1$, where $c \geq 4$ is a fixed even integer.

4. Nonsoluble groups

In this section we use Proposition 3.1 to establish Theorem 1 for nonsoluble groups. More precisely, we prove

PROPOSITION 4.1. *Let G be a finite nonsoluble group. Then $\delta(G) > |G|/2-1$ if and only if $G = A_5$.*

LEMMA 4.2. *Let G be a finite group and let N be a maximal normal subgroup of G such that $G/N \not\in \{Z_2, Z_3, A_5\}$. Then $\delta(G) \leq |G|/2-1$.*

Proof. By Proposition 3.1 we have $\delta(G/N) \leq |G/N|/2-1$, hence Corollary 2.2 yields $\delta(G) \leq |G|/2-1$. □

LEMMA 4.3. *Let G be a nonsoluble group with a normal subgroup N such that $G/N \cong Z_2$. Then $\delta(G) \leq |G|/2-1$.*

Proof. Since G and N are nonsoluble, Lemmas 2.9 and 2.16 imply that

$$i_2(G) \leq \frac{4}{15}|G|-1, \;\; i_3(G) = i_3(N) \leq \frac{7}{20}|N|-1 = \frac{7}{40}|G|-1,$$

whence $3+3i_2(G)+i_3(G) \leq |G|-1$ and the result follows from Lemma 2.3. □

LEMMA 4.4. *Let G be a nonsoluble group with a normal subgroup N such that $G/N \cong Z_3$. Then $\delta(G) \leq |G|/2-1$.*

Proof. Here Lemmas 2.9 and 2.16 imply that

$$i_2(G) = i_2(N) \leq \frac{4}{15}|N|-1 = \frac{4}{45}|G|-1, \;\; i_3(G) \leq \frac{7}{20}|G|-1$$

and again we get $3+3i_2(G)+i_3(G) \leq |G|$. □

LEMMA 4.5. *Let G be a finite group with a nontrivial normal subgroup N such that $G/N \cong A_5$. Then $\delta(G) \leq |G|/2-1$.*

Proof. As before, it suffices to show that $3+3i_2(G)+i_3(G)\leq|G|$. Note that Lemma 2.16 implies that $i_3(G)\leq 7|G|/20-1$. First suppose N is nonabelian. Then Corollaries 2.5 and 2.6 give $i_2(N)\leq 3|N|/4-1$ and $i_2(Nx)\leq 3|N|/4$ for all involutions $x\in G\setminus N$. Therefore

$$i_2(G)\leq i_2(N)+i_2(G/N)\cdot\frac{3}{4}|N|\leq 16\cdot\frac{3}{4}|N|-1=\frac{1}{5}|G|-1$$

and the result follows since

$$3+3i_2(G)+i_3(G)\leq\frac{3}{5}|G|+\frac{7}{20}|G|-1<|G|.$$

Now assume N is abelian. First consider the case where N is an elementary abelian p-group. Let $Nx=(1,2)(3,4)$ and $Ny=(1,2,3)$ represent the unique classes of elements of order 2 and 3 in $G/N\cong A_5$, with respective class sizes 15 and 20.

First suppose $p>2$. If $i_2(Nx)=|N|$ then Lemma 2.10 indicates that every involution in $G\setminus N$ inverts N elementwise, but this is not possible since x commutes with an involution $z\in G\setminus N$ in the coset $Nz=(1,3)(2,4)$, so xz centralizes N. Therefore, $i_2(Nx)<|N|$, hence $i_2(Nx)\leq|N|/3$ (see Lemma 2.7) and thus

$$3+3i_2(G)+i_3(G)\leq 3+3\cdot 15\cdot\frac{1}{3}|N|+\frac{7}{20}|G|-1<|G|.$$

Next assume $p=2$. If $x\in C_G(N)$ then $y\in C_G(N)$ (since every element of order 3 in A_5 is a product of two involutions), so $i_3(G)\leq i_3(A_5)=20$ and the result follows since $i_2(G)\leq 16|N|-1$. On the other hand, if $i_2(Nx)<|N|$ then $i_2(Nx)\leq|N|/2$ by Lemma 2.7, so

$$3+3i_2(G)+i_3(G)\leq 3+3\cdot\left(|N|-1+15\cdot\frac{1}{2}|N|\right)+20|N|<|G|.$$

To deal with the general abelian case, let p be a prime which divides $|N|$ and let $M=\{n^p : n\in N\}$. Then M is a characteristic subgroup of N and N/M is an elementary abelian p-group. Now $(G/M)/(N/M)\cong A_5$, so our earlier argument yields $\delta(G/M)\leq|G/M|/2-1$ and thus Corollary 2.2 gives $\delta(G)\leq|G|/2-1$. □

Now Proposition 4.1 follows from Lemmas 4.2 - 4.5.

5. Proof of Theorem 1

In this section we complete the proof of Theorem 1. In view of Proposition 4.1 and Lemma 4.2, we may assume that G is soluble and that any maximal normal subgroup N of G satisfies $G/N\in\{Z_2,Z_3\}$. We will establish Theorem 1 by proving the nonexistence of a minimal counterexample (see Propositions 5.9 and 5.10). To do this, we require several preliminary lemmas which deal with various special cases.

At the end of this section we also establish the precise values of $\delta(G)$ listed in Table 1, and we prove Corollaries 1 and 2.

LEMMA 5.1. *Let G be a finite soluble group with a nontrivial normal subgroup N such that $G/N \cong S_4$. Then $\delta(G) \leq |G|/2-1$.*

Proof. Here $G/N \cong S_4$ has two classes of involutions, with representatives $Nx_1 = (1,2), Nx_2 = (1,2)(3,4)$ and respective class sizes 6 and 3. There is a unique class of elements of order 3, with representative $Ny = (1,2,3)$ and class size 8.

If N is nonabelian then Corollary 2.6 implies that $i_2(G \setminus N) \leq 9 \cdot 3|N|/4$, hence

$$\delta(G) = \delta(N) + i_2(G \setminus N) + \frac{1}{2} i_3(G \setminus N) \leq |N| - 1 + \frac{27}{4}|N| + 4|N| < \frac{1}{2}|G| - 1$$

since $\delta(N) \leq |N|-1$ and $i_3(G \setminus N) \leq 8|N|$.

Next suppose N is an elementary abelian p-group. First assume $p = 2$. If $x_1 \in C_G(N)$ then $y \in C_G(N)$, so $i_3(G) \leq 8$ and the trivial bound $i_2(G) \leq 10|N|-1$ is sufficient since $|G| \geq 48$. Otherwise, $i_2(Nx_1) \leq |N|/2$ (see Lemma 2.7) and the desired result follows since

$$i_2(G) \leq |N| - 1 + 6 \cdot \frac{1}{2}|N| + 3|N| = 7|N| - 1, \;\; i_3(G) \leq 8|N|$$

and $\delta(G) = i_2(G) + i_3(G)/2$.

Now assume $p = 3$. If $x_1 \in C_G(N)$ then $x_2, y \in C_G(N)$ and the bounds $i_2(G) \leq 9$ and $i_3(G) \leq 9|N|-1$ are sufficient. Similarly, if x_1 inverts N elementwise then $x_2, y \in C_G(N)$ and the result follows since $i_2(G) \leq 3 + 6|N|$ and $i_3(G) \leq 9|N|-1$. Finally, if x_1 neither centralizes N nor inverts N elementwise then $i_2(Nx_1) \leq |N|/3$ (see Lemma 2.7) and the bounds

$$i_2(G) \leq 6 \cdot \frac{1}{2}|N| + 3|N| = 6|N|, \;\; i_3(G) \leq 9|N| - 1$$

are good enough. A very similar argument applies if $p \geq 5$ and we leave the details to the reader.

To deal with the general abelian case, let p be a prime which divides $|N|$ and set $M = \{n^p : n \in N\}$. Then N/M is an elementary abelian p-group and the above argument yields $\delta(G/M) \leq |G/M|/2-1$ since $(G/M)/(N/M) \cong S_4$. Now Corollary 2.2 yields $\delta(G) \leq |G|/2-1$ as required. □

LEMMA 5.2. *Let G be a finite soluble group with a nontrivial normal subgroup N such that $G/N \cong S_3 \times S_3$. Then $\delta(G) \leq |G|/2-1$.*

Proof. The group $G/N \cong S_3 \times S_3$ has three classes of involutions, with representatives $Nx_1 = ((1,2),1), Nx_2 = (1,(1,2)), Nx_3 = Nx_1x_2$ and respective class sizes

$3,3$ and 9. Similarly, there are three classes of elements of order 3, with representatives $Ny_1 = ((1,2,3),1), Ny_2 = (1,(1,2,3)), Ny_3 = Ny_1y_2$ and class sizes $2,2$ and 4.

If N is nonabelian then Corollary 2.6 implies that $i_2(G \setminus N) \leq 15 \cdot 3|N|/4$, so $\delta(G) \leq |G|/2 - 1$ since $\delta(N) \leq |N| - 1$ and $i_3(G \setminus N) \leq 8|N|$.

Next suppose N is an elementary abelian p-group. First assume $p = 2$. Suppose $x_3 \in C_G(N)$, so $y_3 \in C_G(N)$. If $x_1, x_2 \in C_G(N)$ then $y_1, y_2 \in C_G(N)$, hence $i_3(G) \leq 8$ and the bound $i_2(G) \leq 16|N| - 1$ is good enough since $|G| \geq 72$. Similarly, if $x_1 \in C_G(N)$ and $x_2 \notin C_G(N)$ then $i_2(G) \leq 13|N| - 1 + 3|N|/2$ (since $i_2(Nx_2) \leq |N|/2$; see Lemma 2.7), $i_3(G) \leq 2|N| + 6$ and again the desired bound follows. On the other hand, if $x_1 \notin C_G(N)$ then $i_2(Nx_1) \leq |N|/2$ and the subsequent bounds

$$i_2(G) \leq |N| - 1 + 3 \cdot \frac{1}{2}|N| + 12|N|, \;\; i_3(G) \leq 4|N| + 4$$

suffice. Finally, if $x_3 \notin C_G(N)$ then $i_2(Nx_3) \leq |N|/2$ and the result follows since

$$i_2(G) \leq |N| - 1 + 6|N| + 9 \cdot \frac{1}{2}|N|, \; i_3(G) \leq 8|N|.$$

Now assume $p = 3$. Since $i_3(G) \leq 9|N| - 1$, it suffices to show that $i_2(G) \leq 13|N|$. Suppose x_3 inverts N elementwise. If x_1 also inverts N then x_2 does not (since $x_3 \notin C_G(N)$), so Lemma 2.7 implies that $i_2(Nx_2) \leq |N|/3$ and thus

$$i_2(G) \leq 9|N| + 3|N| + 3 \cdot \frac{1}{3}|N| = 13|N|$$

as required. The same bound on $i_2(G)$ clearly holds if x_1 does not invert N elementwise. Finally, if x_3 does not invert N elementwise then $i_2(Nx_3) \leq |N|/3$ and thus

$$i_2(G) \leq 9 \cdot \frac{1}{3}|N| + 6|N| = 9|N|.$$

An entirely similar argument applies when $p \geq 5$ and we omit the details.

The general abelian case now follows as in the proof of the previous lemma. □

LEMMA 5.3. *Let G be a finite soluble group with a nontrivial normal subgroup N such that $G/N \cong S_3 \times D_8 \times E$, where $\exp(E) \leq 2$. Then one of the following holds:*

(i) $G \cong S_3 \times D_8 \times F$ *with* $\exp(F) \leq 2$*;*

(ii) $\delta(G) \leq |G|/2 - 1$.

Proof. Here $i_2(G/N) = |G/N|/2 - 1$ and $i_3(G/N) = 2$. If N is nonabelian then Corollary 2.6 implies that $i_2(Nx) \leq 3|N|/4$ for all involutions $x \in G \setminus N$, hence

$$\delta(G) \leq |N| - 1 + \left(\frac{1}{2}|G/N| - 1\right) \cdot \frac{3}{4}|N| + |N| \leq \frac{1}{2}|G| - 1.$$

Now assume N is abelian. Suppose there exists a noncentral involution $Nx \in G/N$ such that $i_2(Nx) < |N|$. Then Lemma 2.7 implies that $i_2(Nx) \leq |N|/2$, hence

$$i_2(G \setminus N) \leq 2 \cdot \frac{1}{2}|N| + (|G/N|/2 - 3)|N| = \frac{1}{2}|G| - 2|N|$$

and (ii) follows since $i_3(G \setminus N) \leq 2|N|$ and $\delta(N) \leq |N| - 1$. Therefore, we may assume that all noncentral involutions $Nx \in G/N$ satisfy $i_2(Nx) = |N|$. Clearly there exist distinct noncentral involutions Nx_1, Nx_2 such that Nx_1x_2 is also a noncentral involution, so x_1x_2 both inverts and centralizes N elementwise, hence N is an elementary abelian 2-group. The noncentral involutions generate G/N, so $G \cong (G/N) \times N \cong S_3 \times D_8 \times (E \times N)$ and (i) holds. □

LEMMA 5.4. *Let G be a finite soluble group with a minimal normal subgroup N such that $G/N \cong S_3$. Then one of the following holds:*

(i) $G \cong D(A)$*, where A is abelian and* $\exp(A) \geq 3$*;*

(ii) $G \cong S_4$*;*

(iii) $\delta(G) \leq |G|/2 - 1$.

Proof. Here N is an elementary abelian p-group, of order p^m say. Let $Nx = (1,2)$ and $Ny = (1,2,3)$ represent the unique classes of elements of order 2 and 3 in $G/N \cong S_3$, with respective class sizes 3 and 2.

First suppose $p = 2$. If $x \in C_G(N)$ then $y \in C_G(N)$ and it follows that $G \cong N \times S_3 \cong D(N \times Z_3)$, so (i) holds. Now assume $x \notin C_G(N)$. If $i_2(Nx) \leq |N|/4$ then $i_2(G) \leq |N| - 1 + 3|N|/4$ and the bound $i_3(G) \leq 2|N|$ is good enough. Therefore, we may assume $i_2(Nx) = |N|/2$. If $i_3(Ny) \leq |N|/2$, which must be the case if m is odd (see the proof of Lemma 2.11(iii)), then the result follows since $i_2(G) = 5|N|/2 - 1$ and $i_3(G) \leq |N|$.

Therefore, we may assume m is even, $i_2(Nx) = |N|/2$ and $i_3(Ny) = |N|$. If $m \geq 4$ then the hypothesis $i_2(Nx) = |N|/2$ implies that there exists a nontrivial $n \in N$ which is centralized by x and x', where $x' \in G \setminus N$ is an involution and xx' has order 3. Then $xx' \in C_G(n)$ and thus $i_3(Ny) < |N|$, a contradiction. Finally, if $m = 2$ then it is easy to see that $G \cong S_4$ and thus (ii) holds.

Next suppose $p = 3$. If x inverts N elementwise then $y \in C_G(N)$ and it follows that $G \cong D(N \times Z_3)$. Otherwise, $i_2(G) \leq 3|N|/3$ and the bound $i_3(G) \leq |N| - 1 + 2|N|$ is sufficient.

An entirely similar argument applies when $p \geq 5$ and we omit the details. □

In the next lemma we refer to the groups $T(r)$ which are defined in the Introduction (see collection (V) in the definition of $\mathcal{L}$).

LEMMA 5.5. *Let G be a finite group with a nontrivial normal elementary abelian 2-subgroup N of index three. Then one of the following holds:*

(i) $G \cong T(r) \times E$ *and* $Z(G) \cong E$*, where* $r \geq 1$ *and* $\exp(E) \leq 2$*;*

(ii) $G \cong Z_3 \times N$.

In particular, either $\delta(G) \leq |G|/2 - 1$*, or* $G \cong T(r)$ *for some* $r \geq 1$.

Proof. Here G is a split extension of N by $\langle x \rangle = Z_3$, where $|N| = 2^n$ for some $n \geq 1$. Let $\psi \in \mathrm{GL}_n(2)$ be the automorphism of N induced by x. If ψ is trivial then (ii) holds, so assume otherwise. Then ψ is $\mathrm{GL}_n(2)$-conjugate to a block-diagonal matrix of the form $[A, \ldots, A, I_{n-2r}]$ (r copies of A), where $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $r \geq 1$. (Indeed, any element of order 3 in $\mathrm{GL}_n(2)$ is conjugate to such a matrix.)

Fix a basis $\{u_1, v_1, \ldots, u_r, v_r, w_1, \ldots, w_{n-2r}\}$ of N so that $\psi = [A, \ldots, A, I_{n-2r}]$ with respect to this basis. Then

$$\begin{aligned} G \cong \langle u_1, v_1, \ldots, u_r, v_r, w_1, \ldots, w_{n-2r}, x \mid u_i^2 = v_i^2 = w_i^2 = x^3 = 1, \\ \text{all pairs of generators commute except } [x, u_i] = u_i v_i,\ [x, v_i] = u_i \rangle \end{aligned}$$

and thus

$$G \cong \langle u_1, v_1, \ldots, u_r, v_r, x \rangle \times \langle w_1, \ldots, w_{n-2r} \rangle \cong T(r) \times E,$$

where $r \geq 1$ and $\exp(E) \leq 2$. It is not difficult to see that $Z(T(r))$ is trivial, whence $Z(G) \cong E$ as claimed.

The bound $\delta(G) \leq |G|/2 - 1$ is clear in case (ii) so let us consider (i). Here $i_2(T(r)) = |T(r)|/3 - 1$ and $i_3(T(r)) = 2|T(r)|/3$ (since $\delta(T(r)) = 2|T(r)|/3 - 1$; see Table 1), hence

$$\delta(G) = \left(\frac{1}{3} + \frac{1}{3|E|} \right) |G| - 1$$

and thus $\delta(G) \leq |G|/2 - 1$ if and only if E is nontrivial. □

LEMMA 5.6. *Let* G *be a finite group with a nontrivial normal abelian* 2*-subgroup* N *of index nine. Then* $\delta(G) \leq |G|/2 - 1$.

Proof. First observe that $i_2(G) = i_2(N) \leq |N| - 1$. If G/N is cyclic then $i_3(G) \leq 3|N|$ so we may as well assume $G/N \cong Z_3 \times Z_3$. Let Nx_i denote the elements of order 3 in G/N, $1 \leq i \leq 8$.

First suppose N is elementary abelian, of order 2^n say. As observed in the proof of the previous lemma, we have $i_3(Nx_i) = 2^{n-\alpha_i}$, where $|C_N(x_i)| = 2^{\alpha_i}$ and each $n - \alpha_i$ is even (or zero). If $x_i \in C_G(N)$ for some i then $i_3(Nx_i) = i_3(Nx_i^2) = 1$, so $i_3(G) \leq 6|N| + 2$ and the result follows. Now assume $x_i \notin C_G(N)$ for all i. If $i_3(Nx_i) = |N|$ for all i then G is a Frobenius group with kernel N and complement $Z_3 \times Z_3$, but this is not possible since a Sylow p-subgroup of a Frobenius complement must be cyclic for any odd prime p (see [3, Theorem 3.1(iv), §10.3], for example). Therefore, $i_3(Nx_k) = i_3(Nx_k^2) < |N|$ for some k. In fact, if n is odd then $i_3(Nx_i) \leq |N|/2$ for all i (since $n - \alpha_i$ is even), hence $i_3(G) \leq 4|N|$ and we are done. Similarly, if n is even then the bound $i_3(Nx_k) < |N|$ implies that $i_3(Nx_k) \leq |N|/4$ and the result follows since $i_3(G) \leq 2|N|/4 + 6|N|$.

To deal with the general case, let $M = \{n^2 : n \in N\}$. Then N/M is an elementary abelian 2-group and the above argument yields $\delta(G/M) \leq |G/M|/2 - 1$ since $(G/M)/(N/M) \cong Z_3 \times Z_3$. The desired result now follows from Corollary 2.2. □

LEMMA 5.7. *Let G be a finite soluble group with a nontrivial normal subgroup N of odd order such that G/N is a nontrivial 2-group. Then one of the following holds:*

(i) *$G \cong D(A)$, where A is abelian and $\exp(A) \geq 3$;*

(ii) *$G \cong S_3 \times S_3$;*

(iii) *$G \cong S_3 \times D_8 \times E$, where $\exp(E) \leq 2$;*

(iv) $\delta(G) \leq |G|/2 - 1$.

Proof. Here G is a split extension of N by a nontrivial 2-subgroup K, and we have

$$\delta(G) = i_2(G) + \delta(N). \tag{5}$$

First suppose $i_2(Nx) < |N|$ for all $x \in K$. Then Lemma 2.8 implies that $i_2(Nx) \leq |N|/3$ and thus

$$i_2(G) \leq i_2(K) \cdot \frac{1}{3}|N| \leq (|K| - 1) \cdot \frac{1}{3}|N| = \frac{1}{3}(|G| - |N|).$$

Now $\delta(N) \leq (|N| - 1)/2$ (maximal if $\exp(N) = 3$), hence (5) yields

$$\delta(G) \leq \frac{1}{3}(|G| - |N|) + \frac{1}{2}(|N| - 1) = \left(\frac{1}{3} + \frac{1}{6|K|}\right)|G| - \frac{1}{2} \leq \frac{5}{12}|G| - \frac{1}{2}$$

and thus (iv) holds since $|G| \geq 6$.

For the remainder we may assume there exists an involution $x \in K$ such that $i_2(Nx) = |N|$, so N is abelian by Lemma 2.4. Now, if $|K| = 2$ then $G \cong D(N)$ and (i) holds, so we may assume $|K| \geq 4$.

For now we will assume that $C_G(N) \leq N$. If $x_1, x_2 \in K$ are distinct involutions such that $i_2(Nx_1) = i_2(Nx_2) = |N|$ then $x_1x_2 \in C_K(N)$ is nontrivial, but this contradicts the hypothesis $C_G(N) \leq N$. Therefore, there is at most one involution $x \in K$ with $i_2(Nx) = |N|$; for any other involution $y \in K$ we have $i_2(Ny) \leq |N|/3$ by Lemma 2.8. This implies that

$$i_2(G) \leq |N| + (i_2(K) - 1) \cdot \frac{1}{3}|N| \leq \frac{1}{3}(|G| + |N|)$$

since $i_2(K) \leq |K| - 1$, and thus (5) yields

$$\delta(G) \leq \frac{1}{3}(|G| + |N|) + \frac{1}{2}(|N| - 1) = \left(\frac{1}{3} + \frac{5}{6|K|}\right)|G| - \frac{1}{2}$$

since $\delta(N) \leq (|N|-1)/2$. In particular, (iv) holds if $|K| \geq 8$.

Next suppose $|K| = 4$ and let us continue to assume $C_G(N) \leq N$. If $K \cong Z_4$ then $\delta(G/N) = |G/N|/2 - 1$ and thus (iv) follows from Corollary 2.2. Therefore, we may assume K is elementary abelian. Let x_1, x_2 and x_3 be the distinct involutions in K, where $x_3 = x_1x_2$ and $i_2(Nx_1) = |N|$. For $i = 2,3$ let Q_i be the set of elements $n \in N$ such that nx_i is an involution. Since N is abelian, each Q_i is a subgroup of N, and the hypothesis $C_G(N) \leq N$ implies that Q_2 and Q_3 are nontrivial. More precisely, we have $N = Q_2 \times Q_3$, $Q_2 = C_N(x_3)$ and $Q_3 = C_N(x_2)$, hence $G \cong D(Q_2) \times D(Q_3)$ and (5) implies that

$$\delta(G) \leq \left(\frac{3}{8} + \frac{1}{4|Q_2|} + \frac{1}{4|Q_3|}\right)|G| - \frac{1}{2} \tag{6}$$

since $\delta(N) \leq (|N|-1)/2$. If $|Q_2| \geq 7$ then one can check that (6) yields $\delta(G) \leq |G|/2 - 1$ since $|Q_3| \geq 3$. By symmetry, the same is true if $|Q_3| \geq 7$, so we may assume $|Q_i| \in \{3,5\}$ for $i = 2,3$. If $|Q_2| = |Q_3| = 5$ then (6) is good enough, while $i_2(G) = 23$ and $\delta(N) = 2$ if $|Q_2| = 3$ and $|Q_3| = 5$ (or vice versa), hence $\delta(G) = 5|G|/12$. Finally, if $|Q_2| = |Q_3| = 3$ then $G \cong S_3 \times S_3$ and (ii) holds.

To complete the proof of the lemma, let us now assume $C_G(N)$ is not contained in N. Then $C_G(N) = N \times L$, where L is a nontrivial normal 2-subgroup of G. If $G = N \times L$ then the bound $\delta(G) \leq |G|/2 - 1$ quickly follows, so let us assume $G \neq N \times L$. Then G/L is a split extension of $NL/L \cong N$ by a nontrivial 2-subgroup $J/L \cong G/NL$, and we claim that

$$C_{G/L}(NL/L) \leq NL/L.$$

To see this, suppose $Lg \in C_{G/L}(NL/L)$. Then for each nontrivial $n \in N$ there exists $l \in L$ such that $g^{-1}ng = ln$, but l must be trivial since n has odd order, L is a 2-group and $[l,n] = 1$. Hence $Lg \in NL/L$ and the claim follows. In particular, we may apply our earlier work to the factor group G/L.

Now, if $|J/L| \geq 8$ then our earlier analysis implies that $\delta(G/L) \leq |G/L|/2 - 1$, so (iv) holds by Corollary 2.2. Next suppose $|J/L| = 4$. As before, if $J/L \cong Z_4$ then our earlier work gives $\delta(G/L) \leq |G/L|/2 - 1$ and again (iv) holds. Therefore, we may assume $J/L \cong Z_2 \times Z_2$. Once again, by our previous analysis, we reduce to the case $G/L \cong S_3 \times S_3$, so Lemma 5.2 implies that $\delta(G) \leq |G|/2 - 1$ and we are done.

Finally, let us assume $|J/L| = 2$, so G is a split extension of $C_G(N) = N \times L$ by $\langle x \rangle \cong Z_2$, where x inverts N elementwise. Let $H = L.\langle x \rangle$ and note that H is a Sylow 2-subgroup of G. If H is elementary abelian then $G \cong N.\langle x \rangle \times L \cong D(N \times L)$ and (i) holds. For the remainder, let us assume H is not elementary abelian, so $i_2(H) \leq 3|H|/4 - 1$ by Corollary 2.5. Now, if L is elementary abelian then

$$i_2(H \setminus L) = i_2(H) - i_2(L) \leq \frac{3}{4}|H| - 1 - (|L| - 1) = \frac{1}{4}|H|$$

so

$$i_2(G \setminus (N \times L)) \leq i_2(H \setminus L) \cdot |G : N_G(H)| \leq \frac{1}{4}|H| \cdot |N| = \frac{1}{4}|G|$$

and thus (5) yields

$$\delta(G) \leq |L| - 1 + \frac{1}{4}|G| + \frac{1}{2}(|N| - 1) = \left(\frac{1}{4} + \frac{1}{2|N|} + \frac{1}{4|L|}\right)|G| - \frac{3}{2}.$$

We conclude that $\delta(G) \leq 23|G|/48 - 3/2$ since $|N| \geq 3$ and $|L| \geq 4$ (if $|L| = 2$ then $H = L.\langle x\rangle$ is elementary abelian, which is not the case).

For the remainder, we may assume H and L are not elementary abelian. If $i_2(Lx) = |L|$ then L is abelian (see Lemma 2.4) and x inverts $N \times L$ elementwise, hence $G \cong D(N \times L)$ and (i) holds. Therefore, we may assume $i_2(Lx) < |L|$, so $i_2(Lx) \leq 3|L|/4$ (see Lemma 2.4) and thus

$$i_2(G \setminus (N \times L)) \leq |N| \cdot \frac{3}{4}|L| = \frac{3}{8}|G|.$$

Since $i_2(L) \leq 3|L|/4 - 1$ (see Corollary 2.5) and $\delta(N) \leq (|N| - 1)/2$, (5) gives

$$\delta(G) \leq \frac{3}{4}|L| - 1 + \frac{3}{8}|G| + \frac{1}{2}(|N| - 1) = \left(\frac{3}{8} + \frac{3}{8|N|} + \frac{1}{4|L|}\right)|G| - \frac{3}{2}$$

and thus (iv) holds if $|N| \geq 5$ (again note that $|L| \geq 4$ since H is not elementary abelian). Therefore, we may assume $N = Z_3$. Now, if $i_2(Lx) < 3|L|/4$ or $i_2(L) < 3|L|/4 - 1$ then by (5) we have

$$\delta(G) \leq \frac{3}{4}|L| + \frac{3}{8}|G| - 1 = \frac{1}{2}|G| - 1,$$

so we may assume $i_2(Lx) = 3|L|/4$ and $i_2(L) = 3|L|/4 - 1$.

Now by the main theorem of [18] (and the values of $\delta(G)$ listed in Table 1), it follows that $L \cong D_8 \times E$, where $\exp(E) \leq 2$. Similarly, if $H = L.\langle x\rangle$ then $i_2(H) = 3|H|/4 - 1$ so we also have $H \cong D_8 \times F$, where $\exp(F) \leq 2$. We deduce that $H = L.\langle x'\rangle$, where $x' \in Z(H)$ and x' inverts N elementwise, so

$$G = (N \times L).\langle x'\rangle = N.\langle x'\rangle \times L \cong S_3 \times D_8 \times E$$

and thus (iii) holds. □

LEMMA 5.8. *Let G be a finite soluble group with a minimal normal subgroup N such that $G/N \cong D(A)$, where A is abelian and $\exp(A) \geq 3$. Then one of the following holds:*

(i) G is a 2-group;

(ii) $G \cong D(B)$, where B is abelian and $\exp(B) \geq 3$;

(iii) $G \cong S_3 \times D_8 \times E$, where $\exp(E) \leq 2$;

(iv) $G \cong S_3 \times S_3$;

(v) $G \cong S_4$;

(vi) $\delta(G) \le |G|/2-1$.

Proof. Here N is an elementary abelian p-group. Let H be an index-two subgroup of G containing N such that $H/N \cong A$. Since A is abelian, we have $H/N = H_1/N \times H_2/N$ where H_1/N is a 2-group and H_2/N has odd order. Note that H_1 and H_2 are normal subgroups of G.

First assume $p \ge 3$. Here H_2 has odd order and $G/H_2 \cong (G/N)/(H_2/N)$ is a nontrivial 2-group, so the desired conclusion follows from Lemma 5.7.

For the remainder we may assume N is an elementary abelian 2-group, say $|N| = 2^m$. If A is a 2-group then so is G and thus (i) holds, so we may as well assume $|A|$ is divisible by an odd prime. Suppose $i_2(G\setminus H) > |G|/3$. Then Lemma 2.12 implies that $H = K_1 \times K_2$, where K_1 is a 2-group and $|K_2|$ is odd, so either G is a 2-group (and thus (i) holds), or G is an extension of a group of odd order by a nontrivial 2-group and Lemma 5.7 implies that (ii), (iii), (iv) or (vi) holds.

Therefore, for the remainder of the proof, we may assume $i_2(G\setminus H) \le |G|/3$, so by Lemma 2.1 we have

$$\delta(G) = i_2(G\setminus H) + \delta(H) \le \frac{1}{3}|G| + \delta(N) + |N|\cdot\delta(A) \tag{7}$$

with $\delta(N) = |N|-1$.

Suppose that $|A|$ is divisible by a prime $r \ge 5$, so $A = A_1 \times A_2$, where A_1 is an r-group and $|A_2|$ is coprime to r. Then $\delta(A) = \delta(A_1)+\delta(A_2)$, $\delta(A_1) \le (|A_1|-1)/4$ and $\delta(A_2) \le |A_2|-1$, hence (7) yields

$$\delta(G) \le \left(\frac{1}{3} + \frac{|A_1|+4|A_2|-1}{8|A_1||A_2|}\right)|G|-1.$$

If either $|A_1| \ge 9$ or $|A_2| \ge 2$ then this bound implies that (vi) holds. If $A = Z_7$ then $\delta(A) = 1$ and (7) gives $\delta(G) \le 10|G|/21-1$, so we may assume $A = Z_5$. Here $G/N \cong D_5$ has a unique class of involutions, with representative Nx and class size 5. If $i_2(Nx) = |N|$ then $G \cong N \times D_5 \cong D(N \times Z_5)$, so (ii) holds. On the other hand, if $i_2(Nx) < |N|$ then Lemma 2.7 yields $i_2(Nx) \le |N|/2$, hence $i_2(G) \le |N|-1+5|N|/2$ and thus $\delta(G) \le 9|G|/20-1$ since $i_5(G) \le 4|N|$.

For the remainder, we may assume $A = A_1 \times A_2$ where A_1 is a 2-group (possibly trivial) and A_2 is a nontrivial 3-group. If $\exp(A_1) \ge 4$ then $\delta(A_1) \le 3|A_1|/4-1$ (equality if $A_1 = Z_4 \times E$ with $\exp(E) \le 2$) and thus (7) yields

$$\delta(G) \le \left(\frac{1}{3} + \frac{3|A_1|+2|A_2|-2}{8|A_1||A_2|}\right)|G|-1$$

since $\delta(A_2) \le (|A_2|-1)/2$. Therefore $\delta(G) \le |G|/2-1$ since $|A_1| \ge 4$ and $|A_2| \ge 3$, so we may assume $\exp(A_1) \le 2$.

Next we reduce to the case $A_2 = Z_3$. Suppose $|A_2| \ge 9$. Since $\delta(A_1) \le |A_1|-1$ and $\delta(A_2) \le (|A_2|-1)/2$, one can check that (7) yields $\delta(G) \le |G|/2-3/2$ if A_1

is nontrivial. Therefore, we may assume $A = A_2$ is a 3-group. If $\exp(A) \geq 9$ then $\delta(A) = i_3(A)/2 \leq |A|/6 - 1/2$ and thus (7) implies that (vi) holds. Now suppose A is an elementary abelian 3-group. The case $A = Z_3$ follows from Lemma 5.4 since $D(Z_3) \cong S_3$, so we may assume $|A| \geq 9$.

Here $G/N \cong D(A)$ has a unique conjugacy class of involutions, represented by Nx, of size $|A|$, and there are precisely $(|A|-1)/2$ classes of elements of order 3, each of size two. If $i_2(Nx) = |N|$ then it is easy to see that $G \cong D(A \times N)$, so (ii) holds. Now suppose $i_2(Nx) < |N|$. If $i_2(Nx) \leq |N|/4$ then $i_2(G) \leq |N| - 1 + |A||N|/4$, $i_3(G) \leq (|A|-1)|N|$ and we deduce that (vi) holds. Therefore, we may assume $i_2(Nx) = |N|/2$, so $i_2(G) = |N| - 1 + |A||N|/2$. Since A is noncyclic, there exists an element $y \in G \setminus N$ of order 3 such that $i_3(Ny) < |N|$; this quickly follows from [3, Theorem 3.1(iv), §10.3] (the same argument was used in the proof of Lemma 5.6). In particular, Lemma 2.7 implies that $i_3(G) \leq (|A|-3)|N| + 2|N|/2$, and thus

$$\delta(G) \leq |N| - 1 + |A| \cdot \frac{1}{2}|N| + \frac{1}{2}((|A|-3)|N| + |N|) = \frac{1}{2}|G| - 1.$$

To complete the proof, we may assume $A = A_1 \times Z_3$ where A_1 is an elementary abelian 2-group of order 2^n, $n \geq 1$. Recall that $H/N = H_1/N \times H_2/N \cong A_1 \times Z_3$, so $H = H_1H_2$ and the H_i are normal subgroups of G. Note that H_1 is the unique Sylow 2-subgroup of H and $i_3(G) = i_3(H_2) \leq 2|H_2|/3$ since $H_2 = N.Z_3$. Also recall that we may assume $i_2(G \setminus H) \leq |G|/3$, hence

$$\delta(G) = i_2(H) + i_2(G \setminus H) + \frac{1}{2}i_3(G) \leq i_2(H_1) + \frac{1}{3}|G| + \frac{1}{3}|H_2|. \qquad (8)$$

First assume H_1 is not elementary abelian. Then Corollary 2.5 implies that $i_2(H_1) \leq 3|H_1|/4 - 1 = |G|/8 - 1$ (since $|G : H_1| = 6$), hence (vi) follows from (8) if $|A_1| \geq 4$. Now suppose $|A_1| = 2$. If there exists an involution in $H_1 \setminus N$ then $H_1 = N.Z_2$ is a split extension. Moreover, $Z(H_1) \cap N$ is a nontrivial normal subgroup of G, so $N \leq Z(H_1)$ since N is a minimal normal subgroup of G. Therefore $Z(H_1) = N$ or H_1, but both possibilities imply that H_1 is elementary abelian, a contradiction. Therefore, $i_2(H_1) = i_2(N) = |G|/12 - 1$ and (vi) follows from (8).

Now assume H_1 is elementary abelian. Here $H = H_1.Z_3$ so Lemma 5.5 implies that $H = T(r) \times E$ or $Z_3 \times H_1$, where $r \geq 1$ and $\exp(E) \leq 2$. In the latter case, G is an extension of Z_3 by a nontrivial 2-group and Lemma 5.7 applies. Therefore we may assume $H = T(r) \times E$. Now all elements of order 3 in H are contained in H_2, hence $T(r) \leq H_2$ since $T(r)$ is generated by elements of order 3 (this is clear since $i_3(T(r)) = 2|T(r)|/3$). Therefore $H_2 = T(r) \times (E \cap H_2)$ and $E \cap H_2$ is a normal subgroup of G contained in N. By the minimality of N, $E \cap H_2$ is either trivial, or equal to N. The latter possibility is absurd since $H_2 = N.Z_3$, so $E \cap H_2$ is trivial and thus $H_2 = T(r)$.

It follows that $H = H_2 \times E$ with E normal in G and $\exp(E) \leq 2$. Now NE/E is a minimal normal subgroup of G/E and we have $(G/E)/(NE/E) \cong S_3$. Therefore Lemma 5.4 implies that either $\delta(G/E) \leq |G/E|/2 - 1$, $G/E = D(B)$ or $G/E =$

S_4, where B is abelian and $\exp(B) \geq 3$. In the first case, Corollary 2.2 yields $\delta(G) \leq |G|/2-1$, while Lemma 5.1 deals with the case $G/E = S_4$. Finally, suppose $G/E = D(B)$. Now $H/E = H_2 = N.Z_3$ is a subgroup of G/E, so Z_3 is contained in B and thus Z_3 is normal in $D(B)$ (any subgroup of B is normal in $D(B)$). Therefore Z_3 is normal in H_2, so G is an extension of Z_3 by a nontrivial 2-group and thus Lemma 5.7 applies. □

We are now in a position to complete the proof of Theorem 1. Suppose G is a finite soluble group of minimal order such that $\delta(G) > |G|/2-1$ and $G \notin \mathcal{L}$, where $\mathcal{L}$ denotes the collection of groups labelled (I)-(X) in the Introduction. Let N be a maximal normal subgroup of G and note that $G/N \in \{Z_2, Z_3\}$ by Lemma 4.2. We consider both cases in turn.

PROPOSITION 5.9. *The case $G/N = Z_2$ leads to a contradiction.*

Proof. Suppose G has a normal subgroup N of index two. Let $K = \bigcap_i N_i$ be the intersection of all normal subgroups N_i of G such that G/N_i is a 2-group. Then G/K is a nontrivial 2-group and K is nontrivial since all 2-groups with $\delta(G) > |G|/2-1$ are in $\mathcal{L}$ by the main theorem of [18].

Let K_1 be maximal among normal subgroups of G properly contained in K. Then K/K_1 is a minimal normal subgroup of G/K_1, so K/K_1 is an elementary abelian p-group, and the definition of K implies that $p > 2$. By Corollary 2.2, we have $\delta(G/K_1) > |G/K_1|/2-1$ and thus Lemma 5.7 implies that one of the following holds:

(i) $G/K_1 \cong D(A)$, where A is abelian and $\exp(A) \geq 3$;

(ii) $G/K_1 \cong S_3 \times D_8 \times E$, where $\exp(E) \leq 2$;

(iii) $G/K_1 \cong S_3 \times S_3$.

Suppose $G/K_1 \cong D(A)$ as in (i). Note that K_1 is nontrivial since we are assuming $G \notin \mathcal{L}$. Let K_2 be minimal among normal subgroups M of G such that G/M is of the form $D(A_2)$, where A_2 is abelian and $\exp(A_2) \geq 3$. Note that K_2 is nontrivial (since K_1 is nontrivial) and let K_3 be maximal among normal subgroups of G properly contained in K_2. Then K_2/K_3 is a minimal normal subgroup of G/K_3, so $\delta(G/K_3) > |G/K_3|/2-1$ and thus Lemma 5.8 (and the minimality of K_2) implies that $G/K_3 \cong S_4, S_3 \times S_3$ or $S_3 \times D_8 \times E$ with $\exp(E) \leq 2$.

Therefore, to complete the proof we may assume G has a nontrivial normal subgroup L such that $G/L \cong S_4, S_3 \times S_3$ or $S_3 \times D_8 \times E$. The latter case is ruled out by Lemma 5.3, so let us consider the other two. Let M be maximal among normal subgroups of G which are properly contained in L. Then L/M is a minimal normal subgroup of G/M and $(G/M)/(L/M) \cong G/L$. Therefore, Lemmas 5.1 and 5.2 imply that $\delta(G/M) \leq |G/M|/2-1$, so $\delta(G) \leq |G|/2-1$ by Corollary 2.2. This final contradiction completes the proof of the proposition. □

PROPOSITION 5.10. *The case $G/N = Z_3$ leads to a contradiction.*

Proof. Suppose G has a normal subgroup N of index three. If $\delta(N) \leq |N|/2 - 1$ then Lemma 2.1 implies that $\delta(G) \leq |G|/2 - 1$ (since $\delta(G/N) = 1$), a contradiction. Therefore, we have $\delta(N) > |N|/2 - 1$ and so $N \in \mathcal{L}$ by the minimality of G. We now consider the various possibilities for N, labelled (I)–(X) in Section 1.

Suppose $N \cong D(A)$ is of type (I). If $\exp(A) \leq 2$ then G is a split extension of an elementary abelian 2-group by Z_3, so Lemma 5.5 implies that either $G \in \mathcal{L}$ or $\delta(G) \leq |G|/2 - 1$, a contradiction. If $\exp(A) > 2$ then A is a characteristic subgroup of N, so A is normal in G and $\delta(G/A) = |G/A|/3$ since $G/A \cong Z_6$. This contradicts Corollary 2.2. Similarly, we can rule out cases (VIII) and (IX) since G has a normal subgroup M with $G/M \cong Z_6$, while Lemma 5.6 deals with (V) as G has a normal abelian 2-subgroup of index 9 in this case. Of course, if N is of type (VI) then G is a 3-group and the hypothesis $\delta(G) > |G|/2 - 1$ implies that $\exp(G) = 3$, so $G \in \mathcal{L}$. Also note that N is not of type (X) since G is soluble.

Next suppose N is of type (II), (III), or (IV), so $N = Y \times E$ with $\exp(E) \leq 2$ and $Y = D_8 \times D_8$, $H(r)$ or $S(r)$, for some positive integer r. We claim that G admits a homomorphism α such that $N\alpha$ is a 2-group, $G\alpha/N\alpha \cong Z_3$ and one of the following holds:

(i) $N\alpha = D_8 \times D_8$; or

(ii) $N\alpha$ has a minimal characteristic (central) subgroup of order 2^n with n odd.

To see this, first observe that G is a split extension of N by $\langle x \rangle = Z_3$, and $N^2 = Y^2 = Z(Y)$ is a characteristic subgroup of N. Moreover, $Z(Y)$ is an $\langle x \rangle$-invariant subgroup of the elementary abelian 2-group $Z(N) = Z(Y) \times E$, so by Maschke's Theorem there exists an $\langle x \rangle$-invariant subgroup K such that $Z(N) = Z(Y) \times K$. Then K is normal in G and $N/K \cong Y$ (since $N = Y \times K$). If N is of type (II) then the natural homomorphism from G to G/K satisfies (i), so we may as well assume N is of type (III) or (IV). Here $|N/K| = |Y| = 2^{2r+1}$. Let L_1 be a characteristic subgroup of N/K, maximal with respect to having order 2^m with $m \geq 0$ even. Then L_1 is a proper subgroup of N/K so there exists a characteristic subgroup L_2 of N/K such that L_2/L_1 is a minimal characteristic subgroup of $(N/K)/L_1$. Now $L_2 > L_1$, so the choice of L_1 implies that L_2/L_1 has order 2^n, with n odd. Therefore, the natural homomorphism from G to $(G/K)/L_1$ satisfies (ii). This justifies the claim.

Let α be the above homomorphism and set $G_1 = G\alpha, N_1 = N\alpha$, so G_1 is a split extension of N_1 by $\langle x' \rangle = Z_3$. In (II), $N_1 = D_8 \times D_8$ does not admit an automorphism of order 3, so $Z(D_8 \times D_8) = Z_2 \times Z_2$ is a central subgroup of G_1. In (III) and (IV), N_1 has a minimal characteristic subgroup $H \leq Z(N_1)$ of order 2^n with n odd. By Lemma 5.5, since n is odd, there is an element $y = y_1y_2 \in H.\langle x' \rangle$ of order 6, with $|y_1| = 3$, $|y_2| = 2$ and $[y_1, y_2] = 1$. Since $G_1 = N_1.\langle y_1 \rangle$, $y_2 \in H$ and $H \leq Z(N_1)$, it follows that $Z(G_1) \cap H$ is nontrivial, hence $H \leq Z(G_1)$ since H is a minimal characteristic subgroup of G_1 (note that N_1 is characteristic in G_1).

In all three cases, we have shown that N_1 contains a nontrivial elementary abelian 2-subgroup L which is central in G_1. Now

$$i_2(G_1) = i_2(N_1) \leq |N_1| - 1 = \frac{1}{3}|G_1| - 1$$

and

$$i_3(G_1) = i_3(G_1/L) \leq 2|N_1/L| \leq | N_1| = \frac{1}{3}|G_1|$$

since $i_3(Lg) = 1$ for all $g \in G_1 \setminus L$ of order 3, and $G_1/L = (N_1/L).Z_3$ with N_1/L a 2-group. We conclude that $\delta(G_1) \leq |G_1|/2 - 1$, and this contradicts Corollary 2.2.

Finally, suppose N is of type (VII), so $N = S_3 \times D_8 \times E$ with $\exp(E) \leq 2$. Then N has a characteristic subgroup M of order 3 such that $N/M \cong H(1) \times F$ with $\exp(F) \leq 2$. Then $N/M < G/M$ is a subgroup of type (III), so the previous analysis implies that $\delta(G/M) \leq |G/M|/2 - 1$, and this contradicts Corollary 2.2. □

We conclude that a minimal counterexample does not exist; the proof of the main statement of Theorem 1 is complete. To close this section, we justify the precise values of $\delta(G)$ listed in Table 1, and we establish Corollaries 1 and 2.

It is entirely straightforward to calculate the precise value of $\delta(G)$ in cases (I), (II) and (VI)–(X), so let us consider (III), (IV) and (V). In [18], Wall calculates that $i_2(H(r)) = 2^{2r} + 2^r - 1$ (see [18, p. 258]) and thus $\delta(G) = |G|/2 + 2^{n+r} - 1$ if G is of type (III), as claimed in Table 1. Next suppose G is of type (IV). Here $S(r) = N.\langle z\rangle = N.Z_2$, where N is an elementary abelian 2-group of order 2^{2r}, and it suffices to show that $i_2(S(r)) = 2^{2r} + 2^r - 1$. By construction, the Jordan form of the matrix $A \in \mathrm{GL}_{2r}(2) \cong \mathrm{Aut}(N)$ corresponding to conjugation by z has exactly r indecomposable blocks, hence the proof of Lemma 2.11(iii) implies that $i_2(Nz) = 2^r$ and thus $i_2(S(r)) = |N| - 1 + 2^r = 2^{2r} + 2^r - 1$ as claimed. Finally, in (V) we have $G = N.\langle z\rangle = N.Z_3$, where N is an elementary abelian 2-group of order 2^{2r}. Now $i_2(G) = |N| - 1$ and $i_3(Nz) = i_3(Nz^2) = |N|$, so $i_3(G) = 2|N|$ and thus $\delta(G) = 2|N| - 1 = 2|G|/3 - 1$ as claimed.

Corollary 1 quickly follows from the values of $\delta(G)$ listed in Table 1. First observe that if A is abelian with $\exp(A) \geq 3$ then $\delta(A) \leq (|A| - 1)/2$, with equality if and only if $\exp(A) = 3$. Therefore, if G is of type (I) and $\exp(A) \geq 3$ then $\delta(G) \leq 3|G|/4 - 1/2$ and equality is possible. In (III) and (IV) we have

$$\delta(G) = \left(\frac{1}{2} + \frac{1}{2^{r+1}}\right)|G| - 1 \tag{9}$$

and thus $\delta(G) \leq 3|G|/4 - 1$, with equality if and only if $r = 1$. The desired bound is clear in each of the remaining cases.

Finally, let us consider Corollary 2. Suppose G is a finite group with $\exp(G) \geq 3$ and $\delta(G) \geq 2|G|/3$. By inspecting Table 1, it is clear that G must be of type (I),

(III) or (IV). Suppose $G = D(A)$, where A is abelian and $\exp(A) \geq 3$, so $\delta(G) = |G|/2 + \delta(A)$. As before, if $\exp(A) = 3$ then $\delta(A) = (|A|-1)/2$ and thus $\delta(G) = 3|G|/4 - 1/2$. Similarly, if $A = Z_4 \times E$ with $\exp(E) = 2$ then $\delta(A) = |A|/2 - 1$, so $\delta(G) = 3|G|/4 - 1$. In all other cases, A has a homomorphic image of the form Z_p ($p \geq 5$ prime), Z_{p^2} ($p \geq 3$ prime), Z_{pq} (p and q distinct primes) or $Z_4 \times Z_4$, and the bound $\delta(A) \leq |A|/3$ quickly follows. Now, if G is of type (III) or (IV) then (9) holds and we deduce that $\delta(G) \geq 2|G|/3$ if and only if $r = 1$ and $|G| \geq 12$. However, these conditions imply that $G \cong D(Z_4 \times E)$ for some nontrivial elementary abelian 2-group E. This proves Corollary 2.

This completes the proof of Theorem 1, together with Corollaries 1 and 2.

6. An application

In this final section we describe an application of Theorem 1 to the study of near-rings. Recall that a near-ring is a set R with two binary operations $+$ and $\cdot$ such that $(R,+)$ is a group (not necessarily abelian) and $\cdot$ is associative and satisfies a single distributive law. Near-rings were first introduced by Dickson in 1905 in the context of near-fields, and H. Neumann (among others) investigated their connections with groups in the 1950s (see [11], for example). We refer the reader to [12] for general background on near-rings.

Near-rings arise naturally in studying functions on a group. Let G be a finite group and let $M_0(G)$ be the set of functions from G to G which fix the identity. Then $M_0(G)$ is a near-ring with respect to the operations $(f+g)(x) = f(x)g(x)$ and $(f \cdot g)(x) = f(g(x))$, where $x \in G$. These near-rings are particularly important since any finite (zero-symmetric) near-ring can be embedded as a subnear-ring of $M_0(G)$ for some finite group G. (Here a near-ring $(R,+,\cdot)$ is *zero symmetric* if $r \cdot 0 = 0 \cdot r = 0$ for all $r \in R$, where 0 is the identity element of the group $(R,+)$.) In this sense, the $M_0(G)$ play a role similar to that of the symmetric groups in group theory.

It is easy to see that a function α generates $M_0(G)$ (as a near-ring) only if α is a bijection. Let n be a positive integer. We say that $M_0(G)$ is *n-gen* if it can be generated by a bijection of order n (order with respect to composition). In [15], it is shown that $M_0(G)$ is 2-gen if and only if $G \neq Z_3$ and $\exp(G) \geq 3$, while the $M_0(G)$ which are 3-gen are determined in [16]. Bounds on the proportion of bijections which generate $M_0(G)$ are obtained by Neumaier in [10].

Let $p \geq 5$ be a prime number and observe that $M_0(G)$ is p-gen only if $|G| > p$ since there are no bijections of order p in $M_0(G)$ if $|G| \leq p$. Let G be a finite group with $|G| > p$. Then the main theorem of [14] states that precisely one of the following holds:

(i) $M_0(G)$ is p-gen;

(ii) $\exp(G) = 2$ and $|G| \not\equiv 1 \bmod p$;

(iii) G belongs to a finite collection of groups, denoted by $\mathcal{D}(p)$.

Rather surprisingly, it turns out that this finite collection $\mathcal{D}(p)$ can be defined in terms of δ. To see this connection, first observe that a bijection $\alpha \in M_0(G)$ generates $M_0(G)$ only if there are no nontrivial proper α-invariant subgroups of G. Indeed, if $H < G$ is such a subgroup then the near-ring generated by α is contained in the maximal subnear-ring $\{f \in M_0(G) : f(H) \subseteq H\}$. Suppose α has order p and $|G|$ is small (relative to p). The idea is that if $\delta(G)$ is sufficiently large then G may have so many subgroups of prime order that it is impossible to define a bijection α which avoids fixing such a subgroup.

More precisely, in [14] it is shown that $\mathcal{D}(p)$ is the disjoint union

$$\mathcal{D}(p) = \mathcal{D}(2,p) \cup \mathcal{D}(3,p),$$

where a group $G \in \mathcal{D}(i,p)$ if and only if G satisfies the three conditions

$$p(i-1) < |G| \leq pi,\ \delta(G) > (i-1)p,\ \exp(G) \geq 3. \tag{10}$$

In particular, $G \in \mathcal{D}(2,p)$ only if $\delta(G) > |G|/2$, while $G \in \mathcal{D}(3,p)$ only if $\delta(G) > 2|G|/3$. Therefore, in view of Theorem 1 (and the $\delta(G)$ values recorded in Table 1), we can determine the groups in the collections $\mathcal{D}(2,p)$ and $\mathcal{D}(3,p)$.

PROPOSITION 6.1. *We can determine the groups in $\mathcal{D}(p)$ for any prime $p \geq 5$.*

If $p = 2$ or 3 then the groups G for which $M_0(G)$ is p-gen are determined by the second author in [15] and [16]. For $p \geq 5$ we have

COROLLARY 6.2. *Let $p \geq 5$ be a prime and let G be a finite group with $|G| > p$. Then $M_0(G)$ is p-gen if and only if the following hold:*

(i) G is not an elementary abelian 2-group with $|G| \equiv 1$ mod p; and

(ii) G is not in $\mathcal{D}(p)$, as specified in Proposition 6.1.

To illustrate the general approach, below we will use Theorem 1 to determine the groups in $\mathcal{D}(p)$, where $p = 2^8 + 1 = 257$. First we record a couple of results on the general nature of the subsets $\mathcal{D}(2,p)$ and $\mathcal{D}(3,p)$.

PROPOSITION 6.3. *We have $|\mathcal{D}(2,p)| \to \infty$ as $p \to \infty$.*

Proof. Suppose $p \geq 5$. Then there exists a unique integer $m \geq 3$ such that $p < 2^m \leq 2p$, and there are precisely $\lfloor (m-1)/2 \rfloor$ distinct pairs of integers (r,n), where $r \geq 1$, $n \geq 0$ and $m = 2r+1+n$. Therefore, $\mathcal{D}(2,p)$ contains precisely $2\lfloor (m-1)/2 \rfloor - 1$ pairwise nonisomorphic groups of types (III) and (IV), hence

$$|\mathcal{D}(2,p)| \geq 2\lfloor (m-1)/2 \rfloor - 1 \geq m-3 > \log_2 p - 3 \tag{11}$$

and the result follows. □

REMARK 6.4. In practice, most of the groups in $\mathcal{D}(2,p)$ are of type $D(A)$ and thus the lower bound in (11) could be improved. However, computer calculation suggests that the size of $\mathcal{D}(2,p)$ grows slowly, perhaps logarithmically with respect to p. For example, we have calculated that $|\mathcal{D}(2,p)| \leq 576$ for all primes p less than 10^6.

PROPOSITION 6.5. *Let $p \geq 5$ be a prime. Then $|\mathcal{D}(3,p)| \leq 2$.*

Proof. Suppose $G \in \mathcal{D}(3,p)$. Then $2p < |G| \leq 3p$ and $\delta(G) > 2p \geq 2|G|/3$. By Corollary 2, we have $G = D(A)$ where either $\exp(A) = 3$ or $A = Z_4 \times E$ with $\exp(E) = 2$. If $\exp(A) = 3$ then $|A| = 3^m$ for some $m \geq 1$, and it is clear that there can be at most one such m so that $2p < |G| \leq 3p$. Similarly, there is at most one possibility for $|E|$ if $A = Z_4 \times E$. We conclude that $|\mathcal{D}(3,p)| \leq 2$. □

Let us now determine the groups in the collection $\mathcal{D}(257)$. Now, if $G \in \mathcal{D}(3,257)$ then the proof of Proposition 6.5 indicates that there exist positive integers a and b such that $|G| = 2.3^a$ or 2^{b+3}. However, the constraint $514 < |G| \leq 771$ (see (10)) rules out such a possibility, hence $\mathcal{D}(3,257)$ is empty.

Now suppose $G \in \mathcal{D}(2,257)$, so $258 \leq |G| \leq 514$ and $\delta(G) \geq 258$. By Theorem 1, G is a group of type (I)–(X). By inspecting Table 1, it is clear that G is not of type (VI)–(X). Suppose G is of type (V). Here $\delta(G) = 2|G|/3 - 1$, so the condition $\delta(G) \geq 258$ implies that $|G| \geq 389$. Now $|G| = 3.2^{2r}$ for some positive integer r, but there is no r such that $389 \leq |G| \leq 514$, so G is not of type (V). Next suppose G is of type (III) or (IV). Then $|G| = 2^{2r+n+1}$ for some $r \geq 2$ and $n \geq 0$, and (9) holds (note that if $r = 1$ then G is isomorphic to a group of type (I)). The bounds on $|G|$ imply that $(r,n) \in \{(2,4),(3,2),(4,0)\}$, so there are 6 possibilities for G:

$$H(2) \times Z_2^4,\ H(3) \times Z_2^2,\ H(4),\ S(2) \times Z_2^4,\ S(3) \times Z_2^2,\ S(4),$$

where Z_2^k denotes the direct product of k copies of Z_2. If G is of type (II) then $|G| = 2^{n+6}$ for some n, so the constraints on $|G|$ imply that $n = 3$, so $G = D_8 \times D_8 \times Z_2^3$ is the only example in (II).

Finally, suppose $G = D(A)$ is a group of type (I). If G is elementary abelian then $G = Z_2^9$ is the only possibility, so let us assume $\exp(A) \geq 3$. Now Corollary 1 implies that $\delta(G) < 3|G|/4$, so $|G| \geq 344$ and it remains to classify the abelian groups A such that $172 \leq |A| \leq 257$, $\exp(A) \geq 3$ and $\delta(G) = |A| + \delta(A) \geq 258$. With the aid of a computer, it is easy to check that there are exactly 27 possibilities for A, up to isomorphism, listed in Table 3. Here we use the notation $(n_1^{a_1}, \ldots, n_k^{a_k})$ to denote the abelian group $Z_{n_1}^{a_1} \times \cdots \times Z_{n_k}^{a_k}$, where $n_1 < n_2 < \ldots < n_k$.

We conclude that $\mathcal{D}(3,257)$ is empty, while $|\mathcal{D}(2,257)| = 6+1+1+27 = 35$.

REMARK 6.6. In view of Corollary 6.2, it would be interesting to investigate the n-gen problem for n a composite integer. Here very little seems to be known at present. One might expect that similar results to those in [14] hold in the prime power case, while we conjecture that there are only finitely many exceptions when

A	$\|G\|$	$\delta(G)$	A	$\|G\|$	$\delta(G)$
$(3^3,9)$	486	283	$(2^2,64)$	512	263
(3^5)	486	364	(4^4)	512	271
$(5^2,10)$	500	282	$(2^2,8^2)$	512	271
$(3,84)$	504	258	$(2,4^2,8)$	512	271
$(6,42)$	504	260	$(2^2,4,16)$	512	271
(255)	510	258	$(2^3,32)$	512	271
(16^2)	512	259	$(2^2,4^3)$	512	287
$(8,32)$	512	259	$(2^3,4,8)$	512	287
$(4,64)$	512	259	$(2^4,16)$	512	287
$(2,128)$	512	259	$(2^4,4^2)$	512	319
$(4,8^2)$	512	263	$(2^5,8)$	512	319
$(2,8,16)$	512	263	$(2^6,4)$	512	383
$(4^2,16)$	512	263	(257)	514	258
$(2,4,32)$	512	263			

TABLE 3. Abelian groups A with $G = D(A) \in \mathcal{D}(257)$ and $\exp(A) \geq 3$

n is divisible by two distinct primes. It would also be interesting to consider the proportion of bijections of prime order p which generate $M_0(G)$, and study related problems concerning the random generation of such near-rings.

References

[1] T. C. Burness, 'Fixed point ratios in actions of finite classical groups, II', *J. Algebra* **309** (2007), 80–138.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*.

[3] D. Gorenstein, *Finite Groups* (Harper & Row, New York, 1968).

[4] P. V. Hegarty, 'Soluble groups with an automorphism inverting many elements', *Math. Proc. R. Ir. Acad.* **105A** (2005), 59–73.

[5] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, volume 129 of *London Math. Soc. Lecture Note Series* (Cambridge University Press, 1990).

[6] R. Lawther, M. W. Liebeck and G. M. Seitz, 'Fixed point ratios in actions of finite exceptional groups of Lie type', *Pacific J. Math.* **205** (2002), 393–464.

[7] H. Liebeck and D. MacHale, 'Groups with automorphisms inverting most elements', *Math. Z.* **124** (1972), 51–63.

[8] W. A. Manning, 'Groups in which a large number of operators may correspond to their inverses', *Trans. Amer. Math. Soc.* **7** (1906), 233–240.

[9] G. A. Miller, 'Non-abelian groups admitting more than half inverse correspondences', *Proc. Nat. Acad. Sci.* **16** (1930), 168–172.

[10] C. Neumaier, 'The fraction of bijections generating the near-ring of 0-preserving functions', *Arch. Math. (Basel)* **82** (2005), 497–507.

[11] H. Neumann, 'Varieties of groups and their associated near-rings', *Math. Z.* **65** (1956), 36–69.

[12] G. Pilz, *Near-rings*, volume 23 of *North-Holland Mathematics Studies* (North-Holland Publishing Co., Amsterdam, 1983).

[13] W. M. Potter, 'Nonsolvable groups with an automorphism inverting many elements', *Arch. Math. (Basel)* **50** (1988), 292–299.

[14] S. D. Scott, 'Generators of Finite Transformation Nearrings', book in preparation.

[15] ———, 'Involution near-rings', *Proc. Edin. Math. Soc.* **22** (1979), 241–245.

[16] ———, 'Transformation near-rings generated by a unit of order three', *Algebra Colloq.* **4** (1997), 371–392.

[17] M. Vaughan-Lee, *The Restricted Burnside Problem*, volume 8 of *London Math. Soc. Monographs* (Oxford University Press, 1993).

[18] C. T. C. Wall, 'On groups consisting mostly of involutions', *Math. Proc. Cambridge Philos. Soc.* **67** (1970), 251–262.

School of Mathematics
University of Southampton
Southampton SO17 1BJ
UK

Department of Mathematics
University of Auckland
Auckland
New Zealand