FINITE GROUPS WITH AN AUTOMORPHISM CUBING A LARGE FRACTION OF ELEMENTS

PETER HEGARTY

ABSTRACT. We investigate the possible structures imposed on a finite group by its possession of an automorphism sending a large fraction of the group elements to their cubes, the philosophy being that this should force the group to be, in some sense, close to abelian. We prove two main theorems. In the first, we completely classify all finite groups with an automorphism cubing more than half their elements. All such groups are either nilpotent class 2 or possess an abelian subgroup of index 2. For our second theorem, we show that if a group possesses an automorphism sending more than $4/15$ of its elements to their cubes, then it must be solvable. The group A_5 shows that this result is best-possible.

Both our main findings closely parallel results of prevous authors on finite groups possessing an automorphism which inverts many group elements. The technicalities of the new proofs are somewhat more subtle, and also throw up a nice connection to a basic problem in combinatorial number theory, namely the study of subsets of finite cyclic groups which avoid non-trivial solutions to one or more translation invariant linear equations.

1. INTRODUCTION

Let n be an integer. A group G is said to be n-abelian if the map $x \mapsto x^n$ is an endomorphism of G. It is a simple observation that, for $n = -1$ or 2, an n-abelian group is abelian. The fact that there exist non-abelian groups of every exponent greater than or equal to three means that this observation does not extend to any other value of n. However, Alperin [A] obtained an elegant classification of n-abelian groups for every $n > 0$, his result being that a group is n-abelian if and only if it is a homomorphic image of a subgroup of the direct product of an abelian group, a group of exponent dividing n and a group of exponent dividing $n - 1$. In particular, for $n = 3$ this implies that a group for which the map $x \mapsto x^3$ is an injective endomorphism must also be abelian.

Suppose $n \in \{-1, 2, 3\}$. For finite groups, the following questions now arise naturally :

1. Is there a constant $c_n < 1$ such that any finite group G possessing an automorphism sending more than $c_n |G|$ elements to their n:th powers is abelian ?

2. More generally, for what constants $c'_n < 1$ can we produce an 'elegant' (in some sense which is generally acceptable) classification of finite groups G possessing an

automophism sending more than $c'_n |G|$ elements to their n:th powers ? The groups appearing in the classification should all, in some sense, be 'close' to abelian.

Regarding Question 1, it is known that $c_{-1} = c_3 = 3/4$ and $c_2 = 1/2$: see [Mil], [Mac1] and [Z] respectively. For each prime p, let $\mathscr{G}_p$ denote the collection of finite groups whose order is divisible by p and by no smaller prime. Restricting attention to groups in $\mathscr{G}_p$ it is also known that $c_n = 1/p$ for each $n \in \{-1, 2, 3\}$ and for every odd p : see [LM2], [L] and [Mac1].

Regarding Question 2, there is also a lot known. For each odd p, complete classifications are known of those groups in $\mathscr{G}_p$ possessing an automorphism which sends exactly $1/p$ of the group elements to their inverses [LM2], squares [L] respectively cubes [DM]. For even order groups there are the following results :

$n = -1$: In what is probably the most significant paper in this area, Liebeck and MacHale [LM1] provided a concise classification of those groups admitting an automorphism which inverts more than half their elements. MacHale and the author [HM] extended this classification to include groups admitting an automorphism which inverts exactly half the group elements, but already here the classification is considerably more detailed.

$n = -2$: the author [H], improving upon results in [Z], classified neatly all even order groups possessing an automorphism squaring more than one-sixth of their elements. I also provided partial information at exactly one-sixth, but not a full classification.

The missing piece in this jigsaw is a classification analogous to those above when $n = 3$. The main purpose of this paper is to provide this missing piece (Theorem 3.1 below). It is important to note here that all the fractions appearing in these classifications (including ours) appear to be optimal, i.e.: a reasonable corresponding description seems impossible for any smaller value of the fraction in question. In this sense, we think that Theorem 3.1 really does put a finishing touch to the body of work outlined above.

The methods introduced in [LM1] provide the basis for much of the subsequent investigations in the papers cited above. Let $n \in \{-1, 2\}$. If an automorhpism α of a group G sends a large fraction of the elements to their n:th powers, then for a large fraction of pairs x, y of elements the relation $x^n y^n = (xy)^n$ holds, and hence $[x, y] = 1$. Liebeck and MacHale exploit this information by focusing attention on a subgroup H of G of maximal order satisfying $h\alpha = h^n \ \forall \ h \in H$, and considering the (right) coset decomposition of H in G. If x is any element of $G \backslash H$ such that $x\alpha = x^n$ then $\{h \in H : (hx)\alpha = (hx)^n\} = C_H(x)$ is a proper subgroup of H, by definition of the latter. These observations form the basis of a counting argument which eventually leads to the kinds of results we refer to above.

For $n = 3$ we want to apply the same type of argument, but we run into an immediate difficulty, namely : the relation $x^3 y^3 = (xy)^3$ does not on its own imply that x and y commute. The main contribution of the present paper is to remove this obstacle to

obtaining results for $n = 3$ which are as good as those for $n \in \{-1, 2\}$. The technical results obtained in Section 2 for this purpose are thus, in my opinion, the real heart of the paper, especially since they establish an unexpected connection between our problem and a fundamental problem in combinatorial number theory, namely the study of sets of integers which contain no non-trivial solutions to one or more translation invariant linear equations. These connections, which may be of independent interest, are summarised in Proposition 2.9 below.

The final classification obtained in Theorem 3.1 is almost identical to the one in [LM1], except for obvious extra conditions on the 3-part of G. This is, in fact, not a surprise, once the machinery in Section 2 has been developed, though the path to the final result is still more difficult than in [LM1]. Section 3 is devoted to the proof of this theorem. To illustrate further the effectiveness of our machinery, we devote Section 4 to a proof of the fact (Theorem 4.1) that a finite group admitting an automorphism sending more than $4/15$:ths of its elements to their cubes must be solvable. This mirrors analogous results for inverses [P] and squares [H], where the corresponding constants are $4/15$ and $7/60$ respectively. Curiously the same group, namely A_5, illustrates that all three constants are optimal.

The final section (Section 5) provides a brief summary of our findings and a discussion of outstanding issues.

2. Preliminary Lemmas and Connections to Number Theory

First let us fix some notation. If G is a finite group and α an automorphism of G, we denote

$$T_{3,\alpha} := \{g \in G : g\alpha = g^3\}$$

and

$$r_3(G, \alpha) := \frac{|T_{3,\alpha}|}{|G|}.$$

If N is an α-invariant subgroup of G, we denote by α_N the restriction of α to N. If, in addition, $N \lhd G$ then the induced automorphism of G/N is denoted α^N.

We reserve the letter H for a subgroup of G contained inside $T_{3,\alpha}$. In Section 3, but not otherwise, we will further reserve H to denote a subgroup of maximum order with this property. For $x, y \in G$, the commutator $x^{-1}y^{-1}xy$ is denoted $[x, y]$. Finally, for $n > 0$, the cyclic group of order n is denoted $\mathbb{Z}_n$.

In the following lemmas, consider a group G and an automorphism α as given. The proofs of the first two results are obvious :

Lemma 2.1. *If $N \lhd G$ is α-invariant, then $r_3(G, \alpha) \leq r_3(G/N, \alpha^N)$.*

Lemma 2.2. *If $x \in T_{3,\alpha}$ then $C_G(x) = C_G(x^3)$. In particular, if $H \subseteq T_{3,\alpha}$ then $(H : C_H(x))$ is not divisible by three.*

The next two results are also easy :

Lemma 2.3. *If $H \subseteq T_{3,\alpha}$, $x \in T_{3,\alpha}$ and $H/C_H(x^2)$ is elementary 2-abelian, then $hx \in T_{3,\alpha} \Leftrightarrow [h, x] = 1$.*

Proof. Suppose $hx \in T_{3,\alpha}$. Then

$$(hx)\alpha = (hx)^3 = h\alpha x\alpha = h^3 x^3,$$

which implies that $h^2 x^2 = (xh)^2$. But our assumptions imply that $[h^2, x^2] = 1$, thus $(xh)^2 = h^2 x^2 = x^2 h^2$, from which it follows that $[h, x] = 1$.   □

Lemma 2.4. *Suppose each of a, b, ab and ba is in $T_{3,\alpha}$. Then $[a, b] = 1$.*

Proof. As in the proof of the previous lemma, we can deduce immediately from our assumptions that

$$a^2 b^2 = (ba)^2, \quad b^2 a^2 = (ab)^2.$$

But then $a^2 b^3 = (ba)^2 b = b(ab)^2 = b^3 a^2$, so $[a^2, b^3] = 1$. But then $[a^2, b] = 1$ by Lemma 2.2, so now $(ba)^2 = a^2 b^2 = b^2 a^2$, thus $[a, b] = 1$.   □

The next result is the crucial one :

Lemma 2.5. *Suppose each of a, b, ab and $a^{-1}b$ is in $T_{3,\alpha}$. Then $[a, b] = 1$.*

Proof. As previously, we can deduce immediately from our assumptions that

$$a^2 b^2 = (ba)^2 \tag{2.1}$$

and

$$a^{-2} b^2 = (ba^{-1})^2. \tag{2.2}$$

From these and the identity

$$[x, yxy^{-1}] = [x^{-1}y]^3 (y^{-1}xy^{-1})^3 (ya^{-1}yxy^{-1})^3$$

it is easily deduced that $bab^{-1} \in C_G(a)$, from which we also deduce, using (2.1), that $a^2 ba \in C_G(b)$. Thus

$$a^2 bab^{-1} \in C_G(a) \cap C_G(b) \supseteq C_G(ab). \tag{2.3}$$

Now, since G is finite, there exists a positive integer n such that $a^n \in C_G(b)$. First suppose n is even, say $n = 2k$. Then, by (2.3), $(a^2 bab^{-1})^k = a^{2k} bab^{-1} \in C_G(b)$, hence $a^k \in C_G(b)$. Thus we may in fact assume n is odd, say $n = 2k + 1$.

Then, using (2.3) again, we have that $(a^2 bab^{-1})^{k+1} = a^{2k+1}(ab)a^{2k+1}a^{-k}b^{-1} \in C_G(ab)$, which implies that $a^{-k}b^{-1} \in C_G(ab)$ and hence that $(ba^k)^3 \in C_G(ab)$.

But (2.3) also implies that $b^{-1}a^2 b = abab^{-1}$, hence that $b^{-1}a^{2k}b = a^k ba^k b^{-1}$, and in turn that $a^{2k}b^2 = (ba^k)^2$. Thus

$$(ba^k)^3 = a^{2k} b^3 a^k \in C_G(ab). \tag{2.4}$$

Furthermore, by Lemma 2.2 we may assume that n is not divisible by three, so that $k = 3l$ or $k = 3l + 2$ for some l.

First suppose $k = 3l$. Then (2.4) says that $a^{6l} b^3 a^{3l} \in C_G(ab)$. But $a^{6l} b^3 a^{3l} = (a^{2l} ba^l)\alpha$ and $ab \in T_{3,\alpha}$, hence

$$a^{2l} ba^l \in C_G(ab), \tag{2.5}$$

by Lemma 2.2. But, going back to (2.3), we have $(a^2 bab^{-1})^l = a^{2l} ba^l b^{-1} \in C_G(ab)$ which, together with (2.5), implies that $b^{-1} \in C_G(ab)$, hence that $[a, b] = 1$ as required.

Alternatively, if $k = 3l + 2$, then $n \equiv -1 \pmod 6$ so $n^2 \equiv 1 \pmod 6$. Thus if we work with n^2 instead of n we will get the same conclusion, namely that $[a, b] = 1$, and so the lemma is proved. $\square$

Remark 2.6. In the above proof we have used the finiteness of G to guarantee that some power of a commutes with b. Hence the proof goes through in any torsion group, for example. But we do not know whether these restrictions are really necessary, or whether the lemma holds in arbitrary groups.

Corollary 2.7. *Suppose each of a, b, ab and $a^{-2}b$ is in $T_{3,\alpha}$. Then $[a, b] = 1$.*

Proof. The assumptions imply that
$$a^2 b^2 = (ba)^2, \quad a^{-4}b^2 = (ba^{-2})^2.$$

Then
$$a^6 = (a^2 b^2)(a^{-4}b^2)^{-1} = baba^3 b^{-1}a^2 b^{-1},$$

and so
$$a^6 b^3 = baba^3 b^{-1}(a^2 b^2) = (ba)^2 a^3 ba = a^2 b^2 a^3 ba,$$

from which it follows that $b^{-2}a \in C_G(a^3 b^3)$. Then Lemma 2.2 implies that, in fact, $b^{-2}a \in C_G(ab)$. But then $(b^{-2}a)(ab) = (ab)(b^{-2}a)$, hence $a^{-2}b^2 = (ba^{-1})^2$, which implies that $a^{-1}b \in T_{3,\alpha}$. Now the result follows from Lemma 2.5. $\square$

Remark 2.8. Another corollary of Lemma 2.5 is that if a, b, ab and $a^2 b$ are all in $T_{3,\alpha}$, then $[a, b] = 1$. This follows immediately from the lemma upon making the variable substitutions $a' := a$, $b' := ab$. Similarly, if $\{a, b, ab, a^3 b\} \subseteq T_{3,\alpha}$ then $[a, b] = 1$. This follows from Corollary 2.7 upon substituting $a' := a^{-1}$, $b' := ab$. We do not know if it is possible to obtain further results like these. One may ask : does there exist any integer $n \notin \{-1, \pm 2, 3\}$ such that, if $\{a, b, ab, a^n b\} \subseteq T_{3,\alpha}$ then one must have $[a, b] = 1$? We suspect that there are no other such n.

Let H be a subgroup of G such that $H \subseteq T_{3,\alpha}$. Thus H is abelian. Let $x \in T_{3,\alpha}$. Then clearly, $\{h \in H : hx \in T_{3,\alpha}\}$ consists of entire cosets in H of $C_H(x)$. Thus the set $Hx \cap T_{3,\alpha}$ may be identified with a subset, which we denote $\mathscr{T}(H, x)$, of the abelian group $H/C_H(x)$. The last two results now immediately yield the following, which establishes the connection referred to earlier between our work and combinatorial number theory :

Proposition 2.9. *For any subgroup $H \subseteq T_{3,\alpha}$ and any $x \in T_{3,\alpha}$, the subset $\mathscr{T}(H, x)$ of the abelian group $H/C_H(x)$, written additively, contains no non-trivial solutions to either of the translation invariant linear equations $a+b = 2c$, $a+2b = 3c$. In particular, it contains no 3-term arithmetic progressions.*

Proof. This follows directly from Lemma 2.5 and Corollary 2.7. Note that a 3-term arithmetic progression is just a solution to $a + b = 2c$ with $a \neq b$ (we allow $a = c$, which can arise in groups of even order). $\square$

Let $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ be any translation invariant linear function, i.e.: $f(x_1, ..., x_n) = \sum_{i=1}^{n} a_i x_i$ where $a_i \in \mathbb{Z}$ and $\sum_{i=1}^{n} a_i = 0$. It is known that if $A \subseteq \mathbb{N}$ has non-zero upper asymptotic density then A must contain a non-trivial solution to

$f(x_1, ..., x_n) = 0$. This is an easy consequence of the celebrated theorem of Szemerédi stating that if $A \subseteq \mathbb{N}$ has non-zero upper asymptotic density, then A contains arbitrarily long arithmetic progressions. For a discussion of these results, inlcuding a formal definition of what is meant by a 'non-trivial solution' of a translation invariant linear equation, see [R]. Note that, for an equation in three variables, like those appearing in Proposition 2.9, non-trivial means simply that x_1, x_2, x_3 are not all equal.

These results have immediate corollaries in finite cyclic groups, namely, as $n \to \infty$, if $A \subseteq \mathbb{Z}_n$ contains no non-trivial solutions to $f(x_1, ..., x_n) \equiv 0 \pmod{n}$, then $|A| = o(n)$. This is, in fact, what we will use in Section 4 of this paper, where the subgroup H will always be a cyclic group generated by a single element of $T_{3,\alpha}$. It is worth noting though, that corresponding results exist for arbitrary finite abelian groups : for an up-to-date treatment of these matters, see for example [GT].

Speaking somewhat informally, Proposition 2.9 and the above results from number theory imply the following : Let G be a finite group possessing an automorphism α for which $r_3(G, \alpha)$ is large. Then either there is a correspondingly large proportion of commuting pairs of group elements after all (as would be the case if we replaced r_3 by r_{-1} or r_2), or most of the elements of $T_{3,\alpha}$ have small order.

3. Proof of Classification Theorem

The purpose of this section is to prove the following theorem :

Theorem 3.1. *The finite group G admits an automorphism α for which $r_3(G, \alpha) > 1/2$ if and only if G has one of the following structures :*

I. *G is abelian and $(|G|, 3) = 1$.*

II. *G is non-abelian with a normal Sylow 3-subgroup S satisfying the following conditions :*
(a) $S \subseteq K$ where $(G : K) = 2$ and K is abelian,
(b) $S \cap Z(G) = \{1\}$.
In particular, if $(|G|, 3) = 1$ then it suffices for G to have an abelian subgroup of index 2.

III. *G is nilpotent class two and $(|G|, 3) = 1$. All Sylow p-subgroups, for $p > 2$, are abelian. The Sylow 2-subgroup S_2 has one of the following structures :*

(i) *$S_2' \cong C_2 = <z>$, say. $S_2/Z(S_2)$ is elementary abelian, generated by $Zx_1, ..., Zx_k$, $Za_1, ..., Za_k$, subject to the following commutator relations :*

$$[x_i, x_j] = [a_i, a_j] = [a_i, x_j] = 1 \quad whenever \ i \neq j, \quad [a_i, x_i] = z.$$

(ii) *$S_2' \cong C_2 \times C_2 = <z_1> \times <z_2>$, say. $S_2/Z(S_2)$ is elementary abelian of order 16, generated by Zx_1, Zx_2, Za_1, Za_2, subject to the following commutator relations :*

$$[x_i, x_j] = [a_i, a_j] = [a_i, x_j] = 1 \quad whenever \ i \neq j, \quad [a_i, x_i] = z_i.$$

First let us deal with the 'if' part of the theorem by constructing an explicit automorphism α of each type of group such that $r_3(G, \alpha) > 1/2$.

I. The map $\alpha : g \mapsto g^3 \; \forall \; g \in G$ is an automorphism and $r_3(G, \alpha) = 1$.

II. If $x \in G \backslash K$ then $(|x|, 3) = 1$ since, if $x^{3^m n} = 1$ then, by normality of S and commutativity of K, we have $x^n \in S \cap Z(G) = \{1\}$. Now fix any choice of $x \in G \backslash K$ and define the map $\alpha : G \to G$ as follows :

$$k\alpha := k^2 x^{-1} k x \; \forall \; k \in K, \quad x\alpha := x^3, \quad (kx)\alpha := k\alpha x \alpha \; \forall \; k \in K.$$

It is easily checked that α is well-defined and thus a homomorphism. Furthermore, α is one-to-one on K since $k^2 x^{-1} k x = 1 \Leftrightarrow x^3 = (xk^{-1})^3 \Leftrightarrow x = xk^{-1} \Leftrightarrow k = 1$, where we have used the fact that $(|g|, 3) = 1$ for all $g \in G \backslash K$. Thus $\alpha \in \mathrm{Aut}(G)$. Finally, it is also easily verified that $T_{3,\alpha} = Kx \sqcup C_K(x)$, hence $r_3(G, \alpha) = \frac{n+1}{2n} > \frac{1}{2}$, where $(K : C_K(x)) = n$.

III. Let A be the abelian subgroup of G generated by $Z(G)$ and $a_1, ..., a_k$. The map $\alpha : G \to G$ defined by

$$(ax_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_k^{\epsilon_k})\alpha := a^3 x_1^{3\epsilon_1} x_2^{3\epsilon_2} \cdots x_k^{3\epsilon_k} \quad \forall \; a \in A, \; \epsilon_i \in \{0, 1\}, i = 1, ..., k,$$

is easily seen to be an automorphism of G such that $r_3(G, \alpha) = \frac{2^k + 1}{2^{k+1}}$. In particular, for groups of type **(ii)** we have $r_3(G, \alpha) = 5/8$. For more details, see [LM1].

Remark 3.2. For each of the groups G in Theorem 3.1, it is easy to show that there is no $\beta \in \mathrm{Aut}(G)$ such that $r_3(G, \beta) > r_3(G, \alpha)$, where α is the automorphism constructed above. See [LM1] for similar remarks.

Now we turn to the 'only if' part of the theorem. Fix a group G and an automorphism α for which $r_3(G, \alpha) > 1/2$. For the remainder of this section, H will denote a subgroup of G of maximum order subject to the condition that $H \subseteq T_{3,\alpha}$. The center of G will be denoted simply by Z.

Lemma 3.3. $H \supseteq Z$.

Proof. By considering a decomposition of G into cosets of Z we see that if $r_3(G, \alpha) > 1/2$ then $Z \subseteq T_{3,\alpha}$. Since $< Z, x > \subseteq T_{3,\alpha}$ for any $x \in T_{3,\alpha}$, maximality of H implies that $H \supseteq Z$. $\qquad \square$

In the notation of Proposition 2.9 let us denote

$$t(H, x) := \frac{|\mathscr{T}(H, x)|}{|H/C_H(x)|}.$$

In this section we only need some very weak consequences of the machinery developed in Section 2, namely :

Lemma 3.4. *Let* $x \in T_{3,\alpha} \backslash H$. *Then* $|Hx \cap T_{3,\alpha}| \leq \frac{1}{2}|H|$. *Hence every right-coset of* H *in* G *intersects* $T_{3,\alpha}$. *In particular,* H *is not properly contained in any other abelian subgroup of* G. *Moreover, if* $Hx \neq Hx^{-1}$ *and* $(H : C_H(x)) = n > 2$ *then* $|Hx \cap T_{3,\alpha}| + |Hx^{-1} \cap T_{3,\alpha}| \leq \frac{2}{n}\left(1 + \frac{1}{4}\lfloor n - 1 \rfloor\right)|H|$.

Proof. By maximality of H, the group $H/C_H(x)$ must be non-trivial. Then it is an elementary consequence of Proposition 2.9 that $t(H, x) \leq 1/2$. This implies the first assertion of the lemma. The second one follows immediately and then the third from the definition of H.

For the final assertion, let $K := C_H(x) = C_H(x^{-1})$ and consider H/K as an additive group. Let

$$S_+ := \mathscr{T}(H, x)\backslash\{0\}, \quad S_- := \mathscr{T}(H, x^{-1})\backslash\{0\}.$$

Lemma 2.5 implies that

$$S_+ \cap (-S_+) = S_- \cap (-S_-) = S_+ \cap S_- = \phi,$$

from which the result follows. $\square$

Let $(G : H) = m$ and

$$G = H \sqcup Hx_2 \sqcup \cdots \sqcup Hx_m \tag{3.1}$$

be a right-coset decomposition of H in G such that $x_i \in T_{3,\alpha}$ for every $i \in \{2, ..., m\}$. Such a decomposition exists by Lemma 3.4. Then

$$r_3(G, \alpha) = \frac{1}{m}\left(1 + \sum_{i=2}^{m} t(H, x_i)\right). \tag{3.2}$$

The next result will set us up nicely for the remainder of the proof of our theorem :

Lemma 3.5. *Assuming $r_3(G, \alpha) > 1/2$ we must have $r_3(G, \alpha) = \frac{n+1}{2n}$ for some $n \in \mathbb{N}$. Moreover, in a right-coset decomposition of H in G as in (3.1), we must have $(H : C_H(x_i)) > 2$ for at most one index i and $\mathscr{T}(H, x_i) = \{0\}$ for every index i.*

Proof. Let there be k indices i for which $(H : C_H(x_i)) > 2$.

CASE I : $k = 0$.

In this case, by (3.2), $r_3(G, \alpha) = \frac{m+1}{2m}$ where $(G : H) = m$. Clearly, $\mathscr{T}(H, x_i) = \{0\}$ whenever $(H : C_H(x_i)) = 2$.

CASE II : $k = 1$.

Suppose $(H : C_H(x_m)) = n > 2$. If $(G : H) = 2$ then Lemma 2.3 implies that $\mathscr{T}(H, x_2) = \{0\}$ and so $r_3(G, \alpha) = \frac{n+1}{2n}$. Otherwise we must have $Hx_m = Hx_ix_j$ for some $i, j < m$ and so $H/C_H(x_m) \cong C_2 \times C_2$. Thus $n = 4$, $\mathscr{T}(H, x_m) = \{0\}$ and $r_3(G, \alpha) = \frac{2m+1}{4m}$.

CASE III : $k = 2$.

Let i, j be the indices such that $(H : C_H(x_i)) = n_i > 2$ and $(H : C_H(x_j)) = n_j > 2$. By Lemma 2.2, in fact $n_i \geq 4$ and $n_j \geq 4$. If neither $Hx_i^2 = Hx_j$ nor $Hx_j^2 = Hx_i$ holds, then Lemma 2.3 implies that $\mathscr{T}(H, x_i) = \mathscr{T}(H, x_j) = \{0\}$ and (3.2) gives $r_3(G, \alpha) \leq 1/2$, a contradiction. Hence, we may assume that $Hx_i^2 = Hx_j$, say. But then, by Lemma 2.2, there is a third coset, namely Hx_i^3, such that $(H : C_H(x_i^3)) > 2$.

Thus CASE III cannot arise.

CASE IV : $k > 2$.

Let $Hy = Hy_1, Hy_2, ..., Hy_k$ be a complete set of cosets of H in G for which $y_i \in T_{3,\alpha}$ and $(H : C_H(y_i)) = n_i \geq 4$. If $y_i^2 \in H$ then $t(H, y_i) = 1/n_i$ by Lemma 2.3, so if this were the case for every $i = 1, ..., k$ then (3.2) would imply that $r_3(G, \alpha) < 1/2$.

Without loss of generality, suppose $y^2 \notin H$. Thus the cosets Hy and Hy^{-1} are distinct. If $(H : C_H(y^2)) = 2$ then Lemma 2.3 and (3.2) again give the contradiction that $r_3(G, \alpha) \leq 1/2$. Thus $Hy^2 = Hy_j$ for some j. But, using both Lemmas 2.3 and 3.4 this time, we'll get the same contradiction if $(H : C_H(y^4)) \leq 2$. In particular, we may assume that $y^4 \notin H$ and hence that the four cosets $Hy, Hy^{-1}, Hy^2, Hy^{-2}$ are distinct. Grouping these in two pairs and using Lemma 3.4 again, we arrive at the same contradiction unless $(H : C_H(y)) = 5$ and $t(H, y) = 2/5$. In this case, maximality of H means that $y^5 \in H$. But then we claim that, in fact, $\mathscr{T}(H, x) = \{0\}$. For if $hy \in T_{3,\alpha}$ then so is $(hy)\alpha^2 = h^9 y^9$, and hence $h^{-1}y^{-1} \in T_{3,\alpha}$. But then $h \in C_H(y)$ by Lemma 2.4.

Thus CASE IV cannot arise either, and so the proof of Lemma 3.5 is complete.   □

Let us call a right coset Hx *exceptional* if $(H : C_H(x)) > 2$. By Lemma 3.5 there is at most one exceptional coset of H in G. Moreover, we have

Corollary 3.6. *Suppose* $(G : H) > 2$. *Then* $h^2 \in Z$ *for all* $h \in H$. *In fact,* $x^2 \in Z$ *whenever* $x \in T_{3,\alpha}$ *and the coset* Hx *is not exceptional. If* $x \in T_{3,\alpha}$ *and* Hx *is exceptional, then* $H/C_H(x) \cong C_2 \times C_2$, $x^2 \in H$ *and* $x^4 \in Z$.

Proof. Lemma 3.5 immediately implies that $h^2 \in Z$ for all $h \in H$. If $x \in T_{3,\alpha}$ and the coset Hx is not exceptional, then the subgroup $< C_H(x), x >$ has the same properties as H, so applying the lemma to it instead yields that $x^2 \in Z$. Suppose Hx is exceptional. If $x^2 \in H$ then $x^4 \in Z$, so suppose $x^2 \notin H$. Then the subgroup $< C_H(x), x >$ has the same properties as H, and so $x^2 \in Z$, a contradiction.   □

Note that if $(G : H) = 2$ then G is of type **I** or **II** in Theorem 3.1. So henceforth we shall always assume that $(G : H) > 2$. We require two further preparatory results before presenting the main body of our argument.

Lemma 3.7. *Suppose that for every possible choice of the subgroup H we have that $H \lhd G$. Then there is an automorphism β of G, possibly different from α, such that $r_3(G, \beta) > 1/2$ and for which any corresponding H_β is an abelian subgroup of maximum order in G. Moreover, G is of type **III** in Theorem 3.1.*

Proof. From Corollary 3.6 we know that $x^2 \in H$ for all $x \in T_{3,\alpha}$. If $H \lhd G$ this implies that $g^2 \in H$ for all $g \in G$. If the same is true for any possible choice of H then, by Lemma 3.5, it follows that $g^2 \in Z$ for all $g \in G$, since Z is just the intersection of all the possible choices for H.

Now let $x \in T_{3,\alpha}$ and I_x be the inner automorphism of G which sends g to $x^{-1}gx$. Since $g^2 \in Z$ for all g, it is easily checked that $gx \in T_{3,\alpha}$ if and only if $g \in T_{3,I_x\alpha}$. Thus $r_3(G, \alpha) = r_3(G, I_x\alpha)$ for any $x \in T_{3,\alpha}$.

Now let A be an abelian subgroup of maximum order in G. Since $r_3(G, \alpha) > 1/2$, there is some coset Ax such that $x \in T_{3,\alpha}$ and $|Ax \cap T_{3,\alpha}| > \frac{1}{2}|A|$. But then $|A \cap T_{3,I_x\alpha}| > \frac{1}{2}|A|$, so $A \subseteq T_{3,\alpha}$ since A is abelian. So we choose $\beta := I_x\alpha$. It remains to show that G is of type **III** in Theorem 3.1. This is highly non-trivial, but the argument parallels entirely that in Section 4 of [LM1], with very minor modifications. We thus omit further details. $\square$

Lemma 3.8. *Suppose that* $(H : Z) = 2$. *Let* $K := Z \cup G \backslash T_{3,\alpha}$. *Then* K *is an abelian subgroup of index 2 in* G.

Proof. The assumption implies that there is no exceptional coset, and hence $x^2 \in Z$ for all $x \in T_{3,\alpha}$, by Corollary 3.6. Thus if a, b and $b^{-1}a$ are each in $T_{3,\alpha}$ then so is $b^2(b^{-1}a) = ba$, and so $[a, b] = 1$ by Lemma 2.5. By maximality of H, it follows that, for any $x \in T_{3,\alpha} \backslash Z$, we have $C_G(x) \cap T_{3,\alpha} = \langle Z, x \rangle$.

To show that K is closed under multiplication, it suffices to show that if $g_1, g_2 \in K$ then $g_2^{-1}g_1 \in K$. Clearly this is the case if either g_1 or g_2 lies in Z. So suppose $\{g_1, g_2\} \subseteq K \backslash Z$. Let $H = \langle Z, h \rangle$. By Lemma 3.5, there exist $x_1, x_2 \in T_{3,\alpha} \backslash Z$ such that $g_i = hx_i$ for $i = 1, 2$. Then $g_2^{-1}g_1 = x_2^{-1}x_1$, and by the above observations, this lies in $T_{3,\alpha}$ if and only if $[x_1, x_2] = 1$, hence if and only if $x_2 \in \langle Z, x_1 \rangle$. But this will imply that either $g_2^{-1}g_1 \in Z$, which is okay, or that $g_2 \in H \backslash Z$, contradicting that $g_2 \in K$.

This proves that K is closed, hence a subgroup of G. Clearly $(G : K) = 2$ and, by its definition, we can write $G = K \sqcup Kx$, where $Kx \subset T_{3,\alpha}$. Then for any $k \in K$ we have that

$$(kx)\alpha = (kx)^3 = k\alpha x\alpha = k\alpha x^3,$$

hence $k\alpha = kx^{-1}kxk$, since $x^2 \in Z$. But since this holds for any choice of x and k, it follows that K is abelian. $\square$

By Lemma 2.1 and Corollary 3.6 the induced automorphism α^Z of G/Z sends more than half its elements to their inverses. By the main result of [LM1] there are the following three possibilities :

(A) G/Z is abelian.

(B) G/Z is nilpotent class two with $(G/Z)' \cong C_2$ or $C_2 \times C_2$, and various other conditions.

(C) G/Z has an abelian subgroup of index 2.

If **(A)** holds then we are done, by Lemmas 3.3 and 3.7. Next we deal with **(B)** by proving

Lemma 3.9. *Let* G *be a group possessing an automorphism* α *for which* $r_3(G, \alpha) > 1/2$. *Suppose that* G *is nilpotent of class at most 3 and that* $(G/Z)'$ *is elementary abelian of order at most 4. Then unless* G *has an abelian subgroup of index 2, the class of* G *is at most 2.*

Note that this will indeed deal with **(B)**, by Lemma 3.7.

Proof. We consider a minimal counterexample to the lemma and obtain a contradiction. By the results in [DM] we know that all Sylow p-subgroups of G, for $p > 2$, are abelian, so we may assume G to be a 2-group. Further, by Lemma 3.7, we may assume that there is a choice of the subgroup H which is not normal in G. We fix such a choice once and for all. In the body of the text to follow, we shall assume that there are no exceptional right cosets of H in G. Some additional technicalities arise otherwise, and these will be indicated by means of footnotes.

Let $N := N_G(H)$. Since G is nilpotent, we have a strict containment $H \subset N$. We consider three cases :

CASE 1 : N contains an abelian subgroup of index 2, but $(N : H) > 2$.
CASE 2 : $(N : H) = 2$.
CASE 3 : N contains no abelian subgroup of index 2.

First consider CASE 1. Let K denote the abelian subgroup of index 2. By Lemma 3.4, K does not contain H, so $(H : K \cap H) = 2$. But $K \cap H = Z(N)$. Since N is α-invariant, we can now apply Lemma 3.8 to it to conclude that it possesses an abelian subgroup L of index 2, possibly different from K. Indeed, $L = (K \cap H) \cup N \backslash T_{3,\alpha}$.

Suppose $L \lhd G$. Let $x \in T_{3,\alpha} \backslash N$ and $h \in Z(N)$. Then $x^{-1}hx \in L$. But $x^{-1}hx \in T_{3,\alpha}$ since $x^2 \in H$ (Corollary 3.6), thus $x^{-1}hx \in L \cap T_{3,\alpha} \subset H$. But $x \notin N$ so if $(H : C_H(x)) = 2$, then $h \in C_H(x)$. Since x was chosen arbitrarily and there is at most one exceptional coset, it follows that $h \in Z$. Thus $(H : Z) = 2$ and so G possesses an abelian subgroup of index 2.

So we may assume that L is not normal in G. In particular, $L \not\supseteq G'$, so $|L \cap G'| \leq \frac{1}{2}|G'|$. But since G has class at most three and $Z \subseteq H$, we see that $G' \subseteq N$ and is abelian. Hence, by definition of L, $|G' \cap T_{3,\alpha}| > \frac{1}{2}|G'|$ and so $G' \subseteq T_{3,\alpha}$ since it is abelian.

Now consider any $x \in T_{3,\alpha} \backslash H$ for which the coset Hx is not exceptional. We shall show that $x \in N$, which would imply that $N = G$, since there is at most one exceptional coset, contradicting our assumptions about H. Let $h \in H$. Then, since $G' \subseteq T_{3,\alpha}$, we have $[h,x]\alpha = [h,x]^3$. But also $[h,x]\alpha = [h\alpha, x\alpha] = [h^3, x^3]$ and, by Corollary 3.6, $[h^3, x^3] = [h,x]$. Thus $[h,x]^2 = 1$ and another application of Corollary 3.6 implies that $h \in C_H(x^{-1}hx)$. But $C_H(x^{-1}hx) \supseteq C_H(x)$. Thus, since $(H : C_H(x)) = 2$, we conclude that if $h \in H\backslash C_H(x)$ then $x^{-1}hx \in C_G(H)$, hence $x^{-1}hx \in H$ by Lemma 3.4. Thus $x \in N$ as required, and this deals with CASE 1.

Now we turn to CASE 2. We have $|N \cap T_{3,\alpha}| \leq \frac{3}{4}|N|$ by Lemma 3.5. On the other hand, Corollary 3.6 and the fact that G is nilpotent of class at most three imply that every conjugate of H lies in $N \cap T_{3,\alpha}$. To avoid a contradiction we must have $(G : N) = 2$, thus $(G : H) = 4$. Write $G = H \sqcup Hx \sqcup Hy \sqcup Hz$, where $x, y, z \in T_{3,\alpha}$ and the cosets Hx and Hy are not exceptional. If $C_H(x) = C_H(y)$ then $(H : Z) = 2$, a contradiction by Lemma 3.8. Otherwise, $(H : Z) = 4$ and, if Hz is exceptional, then $Z = C_H(z)$ so that, in particular, $z^2 \in Z$. Thus, by Corollary 3.6, the group G/Z, of order 16, has at least 8 involutions. In addition :
   (i) G/Z is non-abelian, since G is not of class two,

(ii) G/Z has a non-normal subgroup of order 4, namely H/Z,

(iii) G/Z has no elements of order 8, since G has no abelian subgroup of index two. These various restrictions serve to eliminate all possible structures for G/Z (see [TW]), a contradiction which completes the analysis of CASE 2.

Finally we turn to CASE 3. It is here that we at last will make use of the induction hypothesis. If it were impossible to find $x_1, x_2 \in G\backslash N$ with $C_H(x_1) \neq C_H(x_2)$, then we'd have $(H : Z) = 2$, a contradiction by Lemma 3.8. So choose $x_1, x_2 \in G\backslash N$ with $C_H(x_1) \neq C_H(x_2)$ and such that neither Hx_1 nor Hx_2 is exceptional, and pick any $h \in C_H(x_1)\backslash C_H(x_2)$. Consider the set

$$S_h := \{g \in G : g^{-1}hg \in H\}.$$

We have $N \subset S_h \subset G$, with all containments proper, since $x_1 \in S_h$ and $x_2 \notin S_h$. But the fact that G is nilpotent of class at most three, together with Lemma 3.3, implies that S_h is in fact a subgroup of G. Moreover it is α-invariant, by Corollary 3.6. Clearly S_h satisfies the remaining hypotheses of Lemma 3.9 so, by minimality of G, either S_h has an abelian subgroup of index two or it is nilpotent class two. The former would imply that N also contained an abelian subgroup of index 2, the latter that $H \lhd S_h$. Either way we have a contradiction, so the proof of Lemma 3.9 is complete. $\square$

It remains to prove Theorem 3.1 under assumption **(C)**, that G/Z contains an abelian subgroup of index 2. Let this subgroup be K/Z where $(G : K) = 2$. By Lemma 3.7 we may assume a choice of H which is not normal in G. Further we may assume that $(H : Z) > 2$, as otherwise, by Lemma 3.8, G is clearly of type **II** in Theorem 3.1. We consider two cases :

CASE 1 : $K \supseteq H$.
CASE 2 : $(K : K \cap H) = 2$.

If $K \supseteq H$ then $H \lhd K$ and so $K = N_G(H)$. Let

$$L := \{h \in H : g^{-1}hg \in H \ \forall \ g \in G\}. \tag{3.3}$$

Then L is evidently a subgroup of H. We cannot have $L = H$ since otherwise $H \lhd G$. On the other hand, for any $x \in G\backslash K$ we have that $C_H(x) \subseteq L$. As there must be at least one non-exceptional coset of H outside K, it follows that $(H : L) = 2$. If there is no exceptional coset, then clearly $L = Z$ and so $(H : Z) = 2$, a contradiction. Otherwise, notice that K is nilpotent class two and α-invariant, being the normaliser of H. Thus, by Lemma 3.7, it is of type **III** in Theorem 3.1. In particular, $(K : C_K(k)) \leq 2$ for every $k \in K$. Thus we'll still get the contradiction that $L = Z$, unless $(K : H) = 2$ and $(H : Z) = 4$. So $|G/Z| = 16$ and G is nilpotent. We can assume that

(i) G/Z is of class three, as otherwise G would be of class at most three and we could apply Lemma 3.9,

(ii) G/Z has no elements of order 8, as otherwise G would have an abelian subgroup of index 2, and thus clearly be of type **II** in Theorem 3.1, since it is nilpotent,

(iii) G/Z has a non-normal subgroup of order 4, namely H/Z.
These conditions eliminate all possible structures for G/Z : see [TW]. We have dealt with CASE 1.

Finally, suppose $(K : K \cap H) = 2$. Let $H^* := K \cap H$. Clearly, $H^* \supseteq Z$ and $H^* \lhd G$. In fact $H^* = L$, the latter defined as in (3.3). We can now argue as before, though note that there is an even easier approach : to avoid the contradiction that $(H : Z) = 2$ we'd need to have $(G : N_G(H)) = 2$ and $H = N_G(H) \cap C_G(H^*)$, which together yield the immediate contradiction that $H \lhd G$.

This completes the proof of Theorem 3.1.

4. Solvable Groups

In this section we further illustrate the effectiveness of the machinery developed in Section 2 by proving

Theorem 4.1. *Let G be a finite group admitting an automorphism α for which $r_3(G, \alpha) > 4/15$. Then G is solvable.*

The constant $4/15$ is best-possible, since $r_3(A_5, i) = 4/15$, where i denotes the identity automorphism.

The proof of Theorem 4.1 is by induction on the group order. Unsurprisingly, we shall have recourse to the classification of the finite simple groups in what follows, though the amount of information we draw on is quite limited and which we begin by summarising.

Lemma 4.2. *Let N be a non-abelian finite simple group and A an abelian subgroup of N of maximum order. Then either $|A|^3 < |N|$ or $N = L_2(q)$ for some prime power q, in which case*

$$|N| = q(q^2 - 1)/2, \quad |A| = q, \quad \text{if } q \text{ is odd,}$$
$$|N| = q(q^2 - 1), \quad |A| = q + 1, \quad \text{if } q \text{ is even.}$$

In particular, N has no abelian subgroup of index less than 12, and if N has an abelian subgroup of index less than 144, then $N = L_2(q)$ for some $q \in \{5, 7, 8, 9, 11, 13\}$.

Proof. The first assertion is the main result of [V]. The second follows from a direct computation and the fact (see [CCNPW]) that the only non-abelian simple groups of order at most $\lfloor (143)^{3/2} \rfloor = 1710$ are the groups $L_2(q)$ for $q \in \{5, 7, 8, 9, 11, 13\}$. $\square$

Lemma 4.3. *No non-abelian finite simple group possesses a solvable subgroup of index less than 5. The only non-abelian finite simple groups possessing a solvable subgroup of index at most 14 are the groups $L_2(q)$, for $q \in \{5, 7, 8, 9, 11, 13\}$, plus the group $L_3(3)$.*

Proof. The first assertion follows from the solvability of S_4. For the second assertion, see [CCNPW]. $\square$

In the following table, N is a non-abelian simple group, A an abelian subgroup of maximum order and M a maximal subgroup of index at most 14. The data and notation are taken from [CCNPW].

N	$|N|$	$(N:A)$	M	$(N:M)$
$L_2(5)$	$2^2 \cdot 3 \cdot 5$	12	A_4	5
			D_{10}	6
			S_3	10
$L_2(7)$	$2^3 \cdot 3 \cdot 7$	24	S_4	7
			$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	8
$L_2(9)$	$2^3 \cdot 3^2 \cdot 5$	40	A_5	6
			$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_4$	10
$L_2(8)$	$2^3 \cdot 3^2 \cdot 7$	56	$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_7$	9
$L_2(11)$	$2^2 \cdot 3 \cdot 5 \cdot 11$	60	A_5	11
			$\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$	12
$L_2(13)$	$2^2 \cdot 3 \cdot 7 \cdot 13$	84	$\mathbb{Z}_{13} \rtimes \mathbb{Z}_6$	14
$L_3(3)$	$2^4 \cdot 3^3 \cdot 13$	432	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes (\mathbb{Z}_2 \cdot S_4)$	13

From this table, we can also conclude the following :

Lemma 4.4. *Let N be a non-abelian finite simple group.*

(i) If N possesses a solvable subgroup S such that $(N:S) \leq 14$ and $Z(S) \neq \{1\}$, then $N \cong L_2(5)$.

(ii) If N possesses a Sylow 2-subgroup of index less than 45, then $N \cong L_2(5)$ or $L_2(7)$.

From now on, G denotes a minimal counterexample to Theorem 4.1 : our aim is to obtain a contradiction. We also fix a choice of $\alpha \in \mathrm{Aut}(G)$ such that $r_3(G, \alpha) > 4/15$.

Lemma 4.5. *If G has either an abelian subgroup of index less than 144 or a solvable subgroup of index less than 25, then G has a non-abelian characteristic simple subgroup N with trivial centraliser. Thus G is isomorphic to a subgroup of $\mathrm{Aut}(N)$.*

Proof. By Lemmas 4.2 and 4.3, any group satisfying either of the hypotheses of Lemma 4.5 can possess no subgroup of the form $N \times N$, where N is a non-abelian simple group. In particular, either G itself is simple, or it possesses a proper characteristic subgroup N_1. By Lemma 2.1 and the minimality of G, the factor group G/N_1 must be solvable. Thus N_1 must be insolvable. Repeating this argument, we see that either N_1 is simple or possesses a proper characteristic subgroup N_2. Then N_2 is also characteristic in G, and so must be insolvable by Lemma 2.1. Iteration of the argument must terminate with a characteristic, non-abelian simple subgroup N of G. Then G possesses a subgroup isomorphic to $N \times C_G(N)$. Our hypotheses on G force $C_G(N)$ to be solvable. But then $G/C_G(N)$ cannot be solvable, so $C_G(N) = \{1\}$ by minimality of G and Lemma 2.1. This proves the lemma. $\square$

Our idea to force a contradiction will be to use the information that $r_3(G, \alpha) > 4/15$ to produce a subgroup S of G which is either abelian of small index or solvable with non-trivial center and even smaller index. We then use the lemmas above to reduce the number of possibilities for G to only a very few, which can be eliminated by direct computation. As in the previous section, we will work around a coset decomposition with respect to a subgroup $H \subseteq T_{3,\alpha}$. However, in this section H will always be a cyclic group, rather than a subgroup of maximum order sitting inside $T_{3,\alpha}$. We will make more

forceful use of Proposition 2.9, and to this end we now introduce some more notation :

Let n be a positive integer. We denote by $T(n)$ the maximum size of a subset of $\mathbb{Z}_n$, written additively, which contains no non-trivial solutions to either of the equations $a + b = 2c$, $a + 2b = 3c$. We set $\tau_n := T(n)/n$. Roth's theorem (see [R]) implies that $\tau_n \to 0$ as $n \to \infty$. We have the following table of values :

n	$T(n)$	τ_n
2	1	$1/2$
4	2	$1/2$
5	2	$2/5$
7	2	$2/7$
8	2	$1/4$
10	2	$1/5$
11	2	$2/11$
13	3	$3/13$
14	3	$3/14$
16	4	$1/4$
17	4	$4/17$

Also it is not difficult to verify that $\tau_n < 4/17$ for any $n > 17$. The proof of Theorem 4.1 will now be accomplished in a sequence of steps, the goal of which is to progressively restrict the possible orders of the elements in the subset $T_{3,\alpha}$ of our hypothetical counterexample G. At the end of this sequence of steps we will be able to conclude that every element of $T_{3,\alpha}$ has order 2 or 4. But then sending an element to its cube is the same as sending it to its inverse, so Theorem 4.1 follows from the analogous result in [P].

Step 1 : $T_{3,\alpha}$ *contains no element of prime power order q where $q \geq 17$.*

The arguments in this first step will provide a protoype for all remaining steps, so we present a careful reasoning here and later on become more concise. Let $h \in T_{3,\alpha}$ be an element of prime-power order q and $H := < h >$. We consider a decomposition of G into right cosets of H and let S be the subgroup of G generated by all the cosets Hx such that $Hx \cap T_{3,\alpha} \neq \phi$ and $C_H(x) \neq \{1\}$. Then $Z(S)$ is non-trivial, since q is a prime power. Also S is α-invariant. Let $(G : S) := r$ and $r_3(G, \alpha) := \xi$. By Proposition 2.9, if $x \notin S$ then $|Hx \cap T_{3,\alpha}| \leq \tau_q|H|$. It follows that $r_3(G, \alpha) \leq \frac{\xi}{r} + \left(1 - \frac{1}{r}\right)\tau_q$ and hence, since $r_3(G, \alpha) > 4/15$ we must have

$$r < \frac{\xi - \tau_q}{4/15 - \tau_q}. \tag{4.1}$$

This is a non-trivial restriction whenever $\tau_q < 4/15$. Then in particular we must have $r_3(S, \alpha_S) > 4/15$ so, by minimality of G, either S is solvable or $S = G$. But the latter contradicts minimality of G, by Lemma 2.1, since $Z(S) \neq \{1\}$. So we conclude that if

$\tau_q < 4/15$ then G contains a solvable subgroup S with non-trivial center and of index bounded by (4.1).

Now, as previously noted, if $q \geq 17$ then $\tau_q \leq 4/17$. Since $\xi \leq 1$ a priori, we then have, by (4.1), that $(G : S) \leq 24$. But, moreover, by Theorem 3.1, if S is non-abelian then $\xi \leq 3/4$ and then (4.1) gives that $(G : S) \leq 16$. So suppose S is non-abelian. Since it is α-invariant and solvable, so also is $S^* := \mathrm{Core}_G(S)$ and G/S^* is isomorphic to a subgroup of S_{16}. But minimality of G and Lemma 2.1 force S^* to be trivial, hence G itself is isomorphic to a subgroup of S_{16}, contradicting the fact that G possesses an element of prime power order $q \geq 17$.

Thus S must be abelian, i.e.: G possesses an abelian subgroup of index at most 24. By Table 1 and Lemma 4.5, G must then be isomorphic to one of $L_2(5)$, S_5 and $L_2(7)$. One checks by direct calculation that none of these three groups possess an automorphism α such that $r_3(G, \alpha) > 4/15$.

Step 2 : $T_{3,\alpha}$ possesses no elements of order 13.

Suppose $h \in T_{3,\alpha}$ with $|h| = 13$. Let $H := <h>$ and consider the subgroup S defined in analogous manner to the previous step. Since $\tau_{13} = 3/13$, we obtain from (4.1) that either S is abelian and $(G : S) \leq 21$ or S is at least solvable with non-trivial center and $(G : S) \leq 14$. The former possibility is dealt with as above. The latter implies, as above, that G can be embedded in S_{14}. But then the subgroup H must be self-centralising in G, so $H = S$ and $|G| \leq 13 \times 14 = 182$. This leaves the same three possibilities for G, by Lemma 4.5, which have already been dealt with.

Step 3 : $T_{3,\alpha}$ possesses no elements of order 11.

Suppose otherwise with $H = <h>$ and $|h| = 11$. Since $\tau_{11} = 2/11$, this time (4.1) yields $(G : S) \leq 9$ so that G is embeddable in S_9, immediately contradicting the existence of any element of order 11 in G.

Step 4 : $T_{3,\alpha}$ possesses no elements of order 16.

Suppose otherwise and let $H = <h>$ with $h \in T_{3,\alpha}$ and $|h| = 16$. Since $\tau_{16} = 1/4 < 4/15$ we could proceed as before, but we would be left with a greater number of possibilities for G to check directly. So we modify our approach. One can check that, up to automorphisms, the only four-element subsets of $\mathbb{Z}_{16}$ that avoid non-trivial solutions to both $a + b = 2c$ and $a + 2b = 3c$ are

$$\{0, 1, 4, 5\}, \quad \{0, 1, 4, 13\}, \quad \{0, 1, 5, 12\}, \quad \{0, 1, 12, 13\}.$$

The important point is that each of these sets contains either 4 or 12. Since the subset $\{4, 12\}$ is characteristic in $\mathbb{Z}_{16}$, it now follows from Lemmas 2.4 and 2.5 that, for any $x \in T_{3,\alpha}$,

$$|Hx \cap T_{3,\alpha}| + |Hx^{-1} \cap T_{3,\alpha}| \leq \frac{7}{16}|H|.$$

Note that this applies even if $Hx = Hx^{-1}$. As a result, when applying (4.1), we can replace $\tau_{16} = 1/4$ by the better constant $\tau'_{16} = 7/32$, which will force the subgroup S to be abelian of index 16 in G. Then the only two remaining possibilities for G (namely A_5 and S_5) have already been considered.

At this point we can state that any element of $T_{3,\alpha}$ must have order $2^i 5^k 7^k$, where $i \leq 3$ and $j, k \leq 1$.

Step 5 : $T_{3,\alpha}$ contains no elements of order $10, 14$ or 35.

Let p_1, p_2 be distinct primes and let $h \in T_{3,\alpha}$ be an element of order $p_1 p_2$. If $\tau_{p_i} \leq 1/2$ for $i = 1, 2$, it is easy to see that the argument in **Step 1** can be modified to produce a subgroup S of G of index

$$ r < \frac{\xi - \tau_{p_1 p_2}}{4/15 - \tau_{p_1 p_2}}, $$

which is still solvable, α-invariant and, crucially, possessing non-trivial center. Indeed, $Z(S)$ will contain either h^{p_1} or h^{p_2}.

Now since, in fact, $\tau_n \leq 1/2$ for any $n > 1$, we can indeed apply this argument. Of the numbers $\tau_{10}, \tau_{14}, \tau_{35}$, the largest is $\tau_{14} = 3/14$ and this gives the worst bounds. We find then that either S is abelian of index at most 14, or non-abelian of index at most 10. The former option is subsumed by previous steps. For the latter, we deduce as before that G is embeddable in S_{10}. But then any cyclic subgroup of order 14 is self-centralising, so $|G| \leq 14 \times 10 = 140$, and we're home and dry.

At this point we can assume that any non-identity element of $T_{3,\alpha}$ has order $2, 4, 5, 7$ or 8.

Step 6 : $T_{3,\alpha}$ contains no elements of order 5.

Since $\tau_5 = 2/5 > 4/15$, we cannot apply the method of **Step 1** directly. Let $H = <h>$ with $h \in T_{3,\alpha}$ and $|h| = 5$. I claim that, if $T_{3,\alpha}$ contains no elements of order greater than 8, then for any $x \in T_{3,\alpha}$ with $[h, x] \neq 1$ we have in fact that $\mathscr{T}(H, x) = \{0\}$. Assuming this to be the case, we can then indeed apply the method of **Step 1**, inserting $1/5$ in place of $2/5$ in eq. (4.1). This yields either an abelian subgroup S of index at most 12, which is dealt with as before, or a solvable subgroup S of index at most 8 such that $H \subseteq Z(S)$. In the latter case, G is embeddable in S_8 and so $|C_G(H)| \leq 30$. Thus $|G| \leq 240$ and we obtain no new possibilities for G here either.

It thus remains to prove our claim. Suppose on the contrary that $x \in T_{3,\alpha}$, $[h, x] \neq 1$ and $hx \in T_{3,\alpha}$. Then $(hx)\alpha^2 = h^9 x^9 \in T_{3,\alpha}$. If $|x| \in \{2, 4, 8\}$ this implies that $h^{-1} x \in T_{3,\alpha}$, a contradiction by Lemma 2.5. If $|x| = 5$ it implies that $h^{-1} x^{-1} \in T_{3,\alpha}$, contradicting Lemma 2.4. Finally, if $|x| = 7$ then instead consider $(hx)\alpha^4 = h^{81} x^{81}$. This is in $T_{3,\alpha}$, hence so also is hx^4. But now each of x, hx, hx^4 and hx^7 is in $T_{3,\alpha}$, which contradicts Proposition 2.9 since $(1, 4, 7)$ is an arithmetic progression.

So now every non-identity element of $T_{3,\alpha}$ may be assumed to have order 2, 4, 7 or 8.

Step 7 : $T_{3,\alpha}$ contains no elements of order 7.

We proceed as above. Assume $h \in T_{3,\alpha}$ with $|h| = 7$. Let $x \in T_{3,\alpha}$ and suppose that also $hx \in T_{3,\alpha}$. If $|x| \in \{2, 4, 8\}$ then considering $(hx)\alpha^2 = h^9 x^9$ we have that $h^2 x \in T_{3,\alpha}$, which forces $[h, x] = 1$ by Proposition 2.9. If instead $|x| = 7$ then considering $(hx)\alpha^3 = h^{27} x^{27}$ yields that $h^{-1} x^{-1} \in T_{3,\alpha}$, again forcing $[h, x] = 1$ by Lemma 2.4.

Thus we can run through the method of **Step 1**, replacing $\tau_7 = 2/7$ by the better constant $1/7$. We omit further details.

We now come to the final step. Every element of $T_{3,\alpha}$ may be assumed to have order 2, 4 or 8. In particular, every element of $T_{3,\alpha}$ has 2-power order.

Step 8 : $T_{3,\alpha}$ contains no elements of order 8.

Suppose the contrary and consider the subgroup S produced by the method of **Step 1**. Since $\tau_8 = 1/4$, one easily checks that the following two possibilities arise :

(i) $r_3(S, \alpha) \le 1/2$ and $(G : S) \le 14$.
(ii) $r_3(S, \alpha) > 1/2$ and $(G : S) \le 44$.

First suppose (i) holds. Since $(G : S) < 25$ we can first apply Lemma 4.5 to conclude that G is isomorphic to a subgroup of $\mathrm{Aut}(N)$, where N is a non-abelian simple subgroup of G isomorphic to one of the groups in Table 1. But now each of the groups in this table has outer automorphism group of order at most 4 (see [CCNPW]). Since $Z(S)$ has non-trivial intersection with a cyclic group of order 8, this implies that the group $N \cap S$ also has a non-trivial center. But then Lemma 4.4(i) implies that $N \cong A_5$, which we've already dealt with.

Finally suppose (ii) holds. Since every element of $T_{3,\alpha}$ has 2-power order, Theorem 3.1 now implies that either S is a 2-group or possesses an abelian subgroup of index 2. In the former case, Lemmas 4.4(ii) and 4.5 leave only the same three possibilies for G which were already encountered in **Step 1**, along with $\mathrm{Aut}(L_2(7))$. This group is also eliminated from consideration by direct calculation. In the latter case, if S is not a 2-group then we must have $r_3(S, \alpha_S) \le 2/3$, so that (4.1) in fact yields $(G : S) \le 24$. Thus G possesses an abelian subgroup of index at most 48, which leaves one more possibility to rule out by direct calculation, namely $L_2(9) \cong A_6$. Having done so, the proof of Theorem 4.1 is complete.

5. Conclusions

By establishing a connection to a well-studied problem in combinatorial number theory, Proposition 2.9 essentially forces one of two alternatives on a finite group G possessing an automorphism which cubes a large fraction of its elements : either a large fraction of pairs of elements in fact commute, or a large fraction of elements have small

order. The connection to number theory may be interesting in its own right for other reasons of which we are not aware. Also intruiging is whether Proposition 2.9 captures the full essence of this connection, or whether there is more to be said. For example one could ask to classify all minimal sets $\mathscr{S}$ of words in two letters a and b such that, if an automorphism of a finite group G cubes every element corresponding to a word in $\mathscr{S}$, then a and b must commute. Are there any such sets other than those identified in Section 2 ? Also intruiging is whether Lemma 2.5 holds in all infinite groups. We leave these matters for future investigation.

ACKNOWLEDGEMENT

REFERENCES

[A]   J. L. Alperin, *A classification of n-abelian groups*, Canad. J. Math. **21** (1969), 1238–1244.

[CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press (1985).

[DM]   M. Deaconescu and D. MacHale, *Odd order groups with an automorphism cubing many elements*, J. Austral. Math. Soc. (Series A) **46** (1989), no. 2, 281–288.

[GT]   B. Green and T. Tao, *An inverse theorem for the Gowers U^3 norm*, http://www.arxiv.org/abs/math/0503014

[H]   P. Hegarty, *On a conjecture of Zimmerman about group automorphisms*, Arch. Math. (Basel) **80** (2003), no. 1, 1–11.

[HM]   P. Hegarty and D. MacHale, *Two-groups in which an automorphism inverts precisely half the elements*, Bull. London Math. Soc. **30** (1998), no. 2, 129–135.

[L]   H. Liebeck, *Groups with an automorphism squaring many elements*, J. Austral. Math. Soc. **16** (1973), 33–42.

[LM1]   H. Liebeck and D. MacHale, *Groups with automorphisms inverting most elements*, Math. Z. **124** (1972), 51–63.

[LM2]   H. Liebeck and D. MacHale, *Groups of odd order with automorphisms inverting many elements*, J. London Math. Soc. (2) **6** (1973), 215–223.

[Mac1]   D. MacHale, *Groups with an automorphism cubing many elements*, J. Austral. Math. Soc. (Series A) **20** (1975), 253–256.

[Mil]   G. A. Miller, *Groups containing the largest possible number of operators of order two*, Amer. Math. Monthly **12** (1905), 149–151.

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

[R]   I. Z. Ruzsa, *Solving a linear equation in a set of integers I*, Acta Arith. **65** (1993), no. 3, 259–282.

[TW]   A. D. Thomas and G. V. Wood, *Group Tables*, Shiva Publishing Limited (1980).

[V]   E. P. Vdovin, Maximal orders of abelian subgroups of finite simple groups, *Algebra and Logic* **38** (1999), no. 2, 67–83.

[Z]   J. Zimmerman, *Groups with automorphisms squaring most elements*, Arch. Math. (Basel) **54** (1990), no. 3, 241–246.

E-mail address: hegarty@math.chalmers.se

Mathematical Sciences, Chalmers University Of Technology and Göteborg University, Göteborg, Sweden