On a conjecture of Zimmerman about group automorphisms

By

Peter V. Hegarty

Abstract

We verify and significantly strengthen a conjecture of Jay Zimmerman about the fraction of elements of a finite group which may be sent to their squares under an automorphism of the group.

Mathematics Subject Classification (1991): 20D45.

1. Introduction. All groups considered are finite. For a group G and $\alpha \in \mathrm{Aut}(G)$, we set

$$S(G,\alpha) = \{g \in G \mid g\alpha = g^2\}. \tag{1}$$

We then set $s(G,\alpha) = \frac{|S(G,\alpha)|}{|G|}$ and define the function $s(G)$ by

$$s(G) = \max_{\alpha \in \mathrm{Aut}(G)} s(G,\alpha). \tag{2}$$

A word on notation : whenever it is clear from the context to which group G we are referring, we will write simply $S(\alpha)$ for $S(G,\alpha)$ and $s(\alpha)$ for $s(G,\alpha)$.

The function $s(G)$ was investigated by Zimmerman in [8], who proved the following result (his notation was slightly different from ours) :

Theorem A. *Suppose $\alpha \in Aut(G)$ with $s(\alpha) \geq \frac{5}{12}$. Then $s(\alpha) = s(G)$ and one of the following holds :*

I. G is abelian of odd order and $s(G) = 1$.

II. G splits over an abelian, odd-order subgroup of index 2, coinciding with $S(\alpha)$ and $s(G) = \frac{1}{2}$.

III. $Z(G)$ is abelian of odd order, $G/Z(G) \cong A_4$ and $G' \cap Z(G) = \{1\}$. In this case, $s(G) = \frac{5}{12}$.

Zimmerman conjectured that if $s(G) > \frac{1}{3}$ then G is soluble. It turns out that the conjecture is true, but that one can prove much stronger results. We prove two theorems. One of these is the complete classification of those groups G of even order such that $s(G) > \frac{1}{6}$, plus a partial classification of those for which $s(G) = \frac{1}{6}$. The number $\frac{1}{6}$ arises naturally, as follows. Clearly, an even order group satisfies $s(G) = l$ if G has an odd order direct factor O of index 2 with $s(O) = 2l$. In [2], Liebeck proved that if G is non-abelian of odd order, then $s(G) \leq \frac{1}{3}$, and he classified all odd order groups where equality holds. Our result is as following :

Theorem B (i) *Let G be a group of even order such that $s(G) \geq \frac{1}{6}$. Let $\alpha \in Aut(G)$ be such that $s(\alpha) \geq \frac{1}{6}$. If $s(\alpha) = s(G)$ then one of the following holds :*

I. $s(G) = \frac{1}{2}$. *G is of type II in Theorem A.*

II. $s(G) = \frac{5}{12}$. *G is of type III in Theorem A.*

III. $s(G) = \frac{1}{4}$. *G has a normal, odd order subgroup of index 4 which coincides with $S(\alpha)$.*

IV. $s(G) = \frac{5}{24}$. *G is a split extension of a group of type II by C_2.*

V. $s(G) = \frac{9}{48}$. *G is a central extension of an odd order subgroup $Z \subset S(\alpha)$ by a group H of order 48. H has a homocyclic, normal Sylow-2 subgroup, which is acted upon fixed-point freely by the elements of H of order 3.*

VI. $s(G) = \frac{25}{144}$. *G is a central extension of an odd order subgroup $Z \subset S(\alpha)$ by $A_4 \times A_4$.*

VII. $s(G) = \frac{1}{6}$. *G has an odd order subgroup of index 2, which is isomorphic to one of the groups of Theorems 4.5 and 4.10 of [2].*

If $s(\alpha) \neq s(G)$, then G is of type I *above, has order divisible by* 3, *and* $s(\alpha) = \frac{1}{6}$.

(ii) *If G is one of the groups of types I through VI above, then G does indeed possess an automorphism α such that $s(\alpha) = s(G) > \frac{1}{6}$.*

In Section 3 we will prove part (i) of this theorem. In Section 4, we will prove part (ii) by giving explicit examples of automorphisms α with the desired properties.

We remark that it seems to be a technically more difficult task to decide which groups of type VII possess an automorphism α with $s(\alpha) = \frac{1}{6}$. We leave the completion of this task for the future. Note that the full classification of even order groups with $s(G) = \frac{1}{6}$ is what's required, together with our result and those of Liebeck [2], to finally obtain the complete analogues of the results of [3] and [4], which give similar classifications of those groups which admit an automorphism sending a large fraction of the group elements to their inverses.

Note, in particular, that all the groups of Theorem B are soluble. This implies Zimmerman's conjecture. It remains to find the smallest possible real number s such that $s(G) > s$ implies G is soluble. Zimmerman noted that $s(A_5, \alpha) = \frac{7}{60}$, where α is conjugation by a transposition in S_5, thus giving a lower bound. We prove

Theorem C. *If $s(G) > \frac{7}{60}$ then G is soluble.*

This result is the correct analogue of Corollary 3.2 of [5], where it was proven that a group possessing an automorphism which sends more than $\frac{4}{15}$ths of the group elements to their inverses is soluble, and that $\frac{4}{15}$ is best-possible. Our proof of Theorem C ultimately relies on the classification of the finite simple groups, which seems to be in the nature of the problem, but is the simplest proof we know of in the sense that we have attempted to minimize our dependence on the classification.

The paper is organised as follows. We prove Theorem C first, in the next section. This result will then be used at one point in the proof of Theorem B, which is given in section 3.

Notation : If $x \in G$, I_x denotes the inner automorphism of G given by

$I_x(g) = x^{-1}gx$. If $\alpha \in \mathrm{Aut}(G)$ and N is a normal, α-invariant subgroup of G, we shall denote by α^* the induced automorphism of G/N. It will always be clear from the context to which normal subgroup α^* refers. We denote by $s'(G/N, \alpha^*)$ the fraction of cosets of N in G which intersect $S(G, \alpha)$. Evidently, we have the inequalities

$$s(G, \alpha) \leq s'(G/N, \alpha^*) \leq s(G/N, \alpha^*). \tag{3}$$

If $x \in S(G, \alpha)$ and H is a subgroup of G, we make the following definitions :

$$H^x = \{h \in H \mid hx \in S(G, \alpha)\}. \tag{4}$$

$$H_x = H^x \cap H^{x^{-1}}. \tag{5}$$

One easily checks the following facts :

$$\text{If } H \lhd G, \text{ then } \mid H^x \mid = \mid H^{x^{-1}} \mid . \tag{6}$$

$$H_x = S(G, \alpha) \cap C_H(x) \text{ and is a subgroup of } H. \tag{7}$$

$$\text{If } H \text{ is abelian, then } H^x \text{ is a subgroup of } H. \tag{8}$$

2. Proof of Theorem C. The following simple result is, so to speak, the key which unlocks the proof. As far as we know, it does not appear in any previous papers on this topic.

Lemma 2.1. *Let G be a group, $\alpha \in Aut(G)$ and A an abelian subgroup of G. Write a coset decomposition $G = \bigsqcup_{i=1}^{n} Ag_i$ where $g_i \in S(\alpha)$ whenever $Ag_i \cap S(\alpha) \neq \phi$. For each such i, put $A^{g_i} := A^i$ for simplicity. Dually, for each $a \in A$, put*

$$n_a = \mid \{i \ : \ a \in A^i\} \mid . \tag{9}$$

Then

$$(i) \qquad \mid S(\alpha) \mid = n_1 + \sum_{a \neq 1} n_a. \tag{10}$$

(ii) For each $a \in A$,

$$(G : C_G(a)) \leq \frac{(G : A)}{n_a}. \tag{11}$$

(iii) If G has trivial soluble radical and p_a is the highest prime divisor of $\mid a \mid$, then

$$p_a + 1 \leq (G : C_G(a)). \tag{12}$$

(iv) If $\mid A \mid > \frac{1}{s(\alpha)}$, there must exist a non-identity element a of A such that

$$(G : C_G(a)) \leq \frac{\mid A \mid \; - 1}{\mid A \mid s(\alpha) \; - \; 1}. \tag{13}$$

Proof. Part (i) is a tautology. Next, note that $a \in A^i \Leftrightarrow \alpha(a) = ag_iag_i^{-1}$. Letting $C = C_G(a)$, if $a \in A^i \cap A^j$ a simple computation shows that $Cg_i = Cg_j$. Since A is abelian, it follows that $(G : C) \leq \frac{(G:A)}{n_a}$, which proves (ii).

Now suppose G has trivial soluble radical and $(G : C) \leq p_a$. Let $X = \mathrm{Core}_G(C)$. Then $(C : X)$ is prime to p_a, so $a^{|a| \, /p_a} \in X$ and $Z(X)$ is a non-trivial, soluble normal subgroup of G. This contradiction proves (iii).

Finally, suppose $(G : C_G(a)) \geq k$ for each non-identity element a of A. By (ii), $n_a \leq \frac{(G:A)}{k}$ for each non-identity element $a \in A$. Since $n_1 \leq \frac{|G|}{|A|}$ (a priori), (10) implies the inequality

$$s(\alpha) \leq \frac{1}{\mid A \mid} + \frac{\mid A \mid \; -1}{k \mid A \mid}, \tag{14}$$

whenever $\mid A \mid s(\alpha) > 1$. This can easily be transformed into (13), which proves (iv).

The idea for the proof of Theorem C is to consider a minimal counterexample G. Henceforth, we reserve the letter G to designate this group. Also fix a choice of an automorphism α of G such that $s(\alpha) > \frac{7}{60}$. The proof is now accomplished by establishing, in succession, the three claims below.

Claim 2.2. *G has trivial soluble radical. It is an extension of a non-abelian, simple normal subgroup S by a subgroup of $Out(S)$. S has order $2^i3^j5^k7^l$, where $i \leq 10$, $j \leq 5$, $k \leq 2$ and $l \leq 1$.*

Our verification of this claim will consist of some elementary arguments, which will also be used to verify Claim 2.3, but will ultimately rely on the following fact from the literature :

Fact 2.2.1 : *There is no non-abelian simple group of any of the following orders :* $13n$ $(n \leq 22)$, $2^n.7.13$, $11n$ $(n \leq 35)$, $2^2.3^n.11$ *or* $2^n.11.m$ $(m \leq 16)$.

Obviously, there is no known easy way to prove this fact - one must use something from the classification of the finite simple groups.

Claim 2.3. *G is, in fact, a simple group, and isomorphic to one of* A_5, A_6, $L_2(7)$ *and* $L_2(8)$.

Proving this will rely on some knowledge of the finite simple groups, specifically on the following facts (notation is taken from the ATLAS [1]):

Fact 2.3.1 : *The non-abelian simple groups of order* $2^i 3^j 5^k 7^l$, *where* $i \leq 10$, $j \leq 5$, $k \leq 2$ *and* $l \leq 1$ *are :* A_n $(5 \leq n \leq 10)$, $L_2(7)$, $L_2(8)$, $U_3(3)$, $U_4(2)$, $L_3(4)$, J_2 *and* $S_6(2)$.

Fact 2.3.2 : *(i) Let S be one of the above groups, other than* A_5, A_6, $L_2(7)$, $L_2(8)$ *and* $L_3(4)$. *Then S has a self-centralizing abelian subgroup of order at least* 12 *and, for any non-identity element x of S,* $(S : C_S(x)) \geq 40$.

(ii) The Sylow-3 subgroups of order 9 *in* $L_3(4)$ *are the centralizers in* $L_3(4)$ *of each of their non-identity elements.*

Fact 2.3.3 : $Out(A_5) \cong Out(L_2(7)) \cong C_2$. $Out(A_6) \cong C_2 \times C_2$ *and* $Out(L_2(8)) \cong C_3$. *The automorphism group of any non-abelian, simple group is complete.*

The reader is invited to check these facts using the ATLAS or GAP etc. The statement about the completeness of the automorphism group of a non-abelian simple group is elementary (see [6], p.452, for example).

Claim 2.4. $s(A_5) = \frac{7}{60}$, $s(A_6) = \frac{17}{360}$, $s(L_2(7)) = \frac{1}{24}$ *and* $s(L_2(8)) = \frac{19}{504}$.

To prove this last claim, which evidently gives the contradiction implying our theorem, requires some explicit and tedious computations which we will not show here. Details may be obtained from the author if desired.

Proof of Claim 2.2. By minimality of G, eq. (3) immediately implies that G has trivial soluble radical. Now we find it convenient to split the remainder of the proof into several steps :

Step 1 : $\pi(G) \subseteq \{2,3,5,7,11,13\}$. $\mid G \mid$ *is not divisible by* 11^2 *or* 13^2.

Proof. Let p be the greatest prime divisor of $\mid G \mid$. Let A be a maximal abelian p-subgroup of G, of order p^n, say. Equations (12) and (13) imply the inequality

$$p+1 \leq \frac{60(p^n-1)}{7p^n-60}, \tag{15}$$

which can only be satisfied if (a) $p \leq 7$, n arbitrary (b) $p = 11$ or 13 and $n = 1$. This proves Step 1.

Step 2 : $13 \notin \pi(S)$.

Proof. Suppose the contrary. Let A be a maximal abelian 13-subgroup of G. By Step 1, $\mid A \mid = 13$. Let $C = C_G(A)$. From (13), we obtain
$(G:C) < \frac{60(13-1)}{7(13)-60} < 24$, so that, in fact, $(G:C) \leq 22$, by Step 1.

Suppose $\mid C \mid$ is divisible by the prime $p \neq 13$. Let x be any element of C of order p and put $B = < A, x >$. Applying Lemma 2.1 to the abelian subgroup B of G, (10) and (11) give the inequality

$$\frac{7}{60} < \frac{1}{13p} + \frac{p-1}{13p(p+1)} + \frac{12p}{13p(G:C)}. \tag{16}$$

Since $(G:C) \geq 14$, this inequality is only satisfiable for $p = 2$ and $(G:C) = 14$. It follows that either (a) C has order 13 and $(G:C) \leq 22$ or (b) $\pi(C) \subseteq \{2,13\}$ and $(G:C) = 14$. In either case, Fact 2.2.1 implies that G has no non-abelian simple subgroup, a contradiction.

Step 3 : $11 \notin \pi(G)$.

Proof. The argument is the same as in Step 2, so we don't give full details. Suppose the contrary and let A be a maximal abelian 11-subgroup of G. Then $\mid A \mid = 11$. Putting $C = C_G(A)$ and using (13), we see that $(G:C) < \frac{60(11-1)}{7(11)-60} < 36$. Suppose $\mid C \mid$ is divisible by the prime $p \neq 11$. Then the relevant inequality obtained from (10) and (11) is only satisfiable if (a) $p = 3$ and $(G:C) = 12$ or (b) $p = 2$ and $(G:C) \leq 16$.

Hence, either (a) $\pi(C) \subseteq \{3, 11\}$ and $(G : C) = 12$ or (b) $\pi(C) \subseteq \{2, 11\}$ and $(G : C) \leq 16$ or (c) $\mid C \mid = 11$ and $(G : C) \leq 35$. In all three cases, Fact 2.2.1 implies that G has no non-abelian, simple subgroups, a contradiction.

Step 4 : (i) G contains no subgroup of the form $S \times T$, where both S and T are non-abelian simple groups.

(ii) Hence, G is an extension of a normal, non-abelian simple subgroup S by a subgroup of Out(S), where $\pi(S) \subseteq \{2, 3, 5, 7\}$.

Proof. (i) Suppose the contrary. By Burnside's theorem, $S \times T$ contains an abelian subgroup $A \times B$ isomorphic to $C_p \times C_q$, for some pair of odd primes p and q, both at least 5, such that $C_p \cong A \subset S$ and $C_q \cong B \subset T$. We write $A \times B$ as the disjoint union of the four subsets U, V, W, X given by $U = 1 \times 1$, $V = A \backslash \{1\} \times 1$, $W = 1 \times B \backslash \{1\}$, $X = A \backslash \{1\} \times B \backslash \{1\}$. Let $\zeta \in A \times B$. If $\zeta \in U$, then $(G : C_G(\zeta)) = 1$. If $\zeta \in V$, then $(G : C_G(\zeta)) \geq (S : C_S(\zeta)) \geq p + 1$, the latter inequality following from the fact that, since S is simple, it possesses no conjugacy class of prime order. Similarly, if $\zeta \in W$, then $(G : C_G(\zeta)) \geq q + 1$. Finally, if $\zeta \in X$, then $(G : C_G(\zeta)) \geq (S \times T : C_{S \times T}(\zeta)) \geq (p + 1)(q + 1)$. By (10) and (11), it follows that the maximum possible value for $s(G, \alpha)$ is

$$\frac{1}{pq} + \frac{p-1}{pq(p+1)} + \frac{q-1}{pq(q+1)} + \frac{(p-1)(q-1)}{pq(p+1)(q+1)}. \qquad (17)$$

One may check that this can never be greater than $\frac{7}{60}$, which proves (i).

(ii) Now let S be a characteristically simple, normal subgroup of G. By (i), S is simple. Then $S \times C_G(S)$ is a subgroup of G. Since G has no non-trivial, soluble normal subgroups, either $C_G(S)$ is trivial or insoluble. But in the latter case, $C_G(S)$ has a non-abelian simple subgroup, contradicting (i). Hence $C_G(S)$ is trivial, which proves that G is an extension of S by a subgroup of Out(S). By Steps 2 and 3, $\pi(S) \subseteq \{2, 3, 5, 7\}$.

Henceforth, we reserve the letter S for the unique normal, non-abelian, simple subgroup of G. The next step will complete the proof of Claim 2.2 :

Step 5 : S has order $2^i 3^j 5^k 7^l$, where $i \leq 10$, $j \leq 5$, $k \leq 2$ and $l \leq 1$.

Proof. Let $p \in \{2, 3, 5, 7\}$ and let A_p be a maximal abelian p-subgroup of S, of order p^{n_p}, say. By (13), there is a non-identity element $x \in A_p$ such that $(S : C_S(x)) \leq (G : C_G(x)) < \frac{60(p^{n_p}-1)}{7p^{n_p}-60}$. Since S is simple, it is therefore a subgroup of $S_{f(p)}$, where $f(p) = \left[\frac{60(p^{n_p}-1)}{7p^{n_p}-60}\right]$. Hence,

$$\mathrm{ord}_p(\mid S \mid) \leq \mathrm{ord}_p(\mid A_{f(p)} \mid). \tag{18}$$

But it is well-known (see, for example, [7], p.94) that

$$\mathrm{ord}_p(\mid S \mid) \leq \frac{1}{2} n_p(n_p + 1). \tag{19}$$

Then one may verify that both of these inequalities can only be satisfied if $\mathrm{ord}_p(\mid S \mid) \leq 10, 5, 2, 1$ according as $p = 2, 3, 5, 7$ respectively, which is what we wanted to show. We illustrate the case $p = 2$ here :

Suppose $\mathrm{ord}_2|S| > 10$. Then (19) implies that $n_2 > 4$, so $n_2 \geq 5$ since n_2 is an integer. Now, for any fixed prime p, the function

$$f_p(x) = \frac{60(p^x - 1)}{7p^x - 60}$$

is strictly decreasing in the domain $x > 0$, as can be verified by computing its' derivative. Hence, if $n_2 \geq 5$, then $f(2) \leq f(5) < 12$. Hence, by (18),

$$\mathrm{ord}_2(\mid S \mid) \leq \mathrm{ord}_2(\mid A_{11} \mid) = 7,$$

contradicting the assumption that $\mathrm{ord}_2|S| > 10$.

Proof of Claim 2.3. S is isomorphic to one of the simple groups listed in Fact 2.3.1. If A is an abelian subgroup of S of order at least 12, then (13) implies the existence of a non-identity element a of A such that $(S : C_S(a)) \leq (G : C_G(a)) < \frac{60(12-1)}{7(12)-60} < 28$. By Fact 2.3.2, S must be isomorphic to one of A_5, A_6, $L_2(7)$, $L_2(8)$ and $L_3(4)$.

If $S \cong L_3(4)$, let A be a Sylow-3 subgroup of S. A is abelian of order 9 so, by (13), there exists a non-identity element $a \in A$ such that
$(S : C_S(a)) \leq (G : C_G(a)) < \frac{60(9-1)}{7(9)-60} = 160$. But $C_S(a) = A$, by Fact 2.3.2, so that $(S : C_S(a)) = \frac{|A|}{9} = \frac{20160}{9} > 160$, a contradiction.

This proves that $S \cong A_5$, A_6, $L_2(7)$ or $L_2(8)$. If $\mathrm{Out}(S)$ is a 2-group then, since $S \lhd G$, it is obvious that $S(G, \alpha) = S(S, \alpha)$. Thus $s(S) \geq s(G)$ and, by minimality of G, we must have $S = G$. If $\mathrm{Out}(S) \cong C_3$ we get the same conclusion, though we need to use the fact that $\mathrm{Aut}(S)$ is complete to deduce that $S(G, \alpha) = S(S, \alpha)$.

Therefore, by Fact 2.3.3, we have established Claim 2.3, and thus completed the proof of Theorem C.

3. Proof of Theorem B, part (i). Again, the proof is by induction on the group order. Trivially, the result holds when $\mid G \mid = 2$, so suppose it holds for groups of even order $< 2k$ and let G be a group of order $2k$ such that $s(G) \geq \frac{1}{6}$. We fix a choice of $\alpha \in \mathrm{Aut}(G)$ such that $s(\alpha) \geq \frac{1}{6}$. Now we divide the proof into two main cases.

Case I : G possesses a non-trivial, normal, α-invariant subgroup of even index.

Fix a choice of such a subgroup and call it N. Since $s(G/N, \alpha^*) \geq \frac{1}{6}$, we may apply the induction hypothesis, and one of six possibilities occurs.

A. G/N is of type I. Then G possesses a normal, α-invariant subgroup M of index 2. Since $S(\alpha) \subseteq M$, we have $s(M, \alpha) \geq \frac{1}{3}$. By the results of [2], either $s(M, \alpha) = \frac{1}{3}$ or $M = S(\alpha)$. Thus, G is either of type I or VII as in the theorem.

B. G/N is of type III. Then G possesses a normal, α-invariant subgroup M of index 4. Since $S(\alpha) \subseteq M$, we have $s(M, \alpha) \geq \frac{2}{3}$. By Theorem A, $M = S(\alpha)$ and G is of type III.

C. G/N is of type V. Then G possesses a normal, α-invariant subgroup M with G/M of order 48 and $s(G/M, \alpha^*) = \frac{9}{48}$. Since $s(\alpha) \geq \frac{1}{6}$, at least 8 cosets of M meet $S(\alpha)$, but the number of such cosets is odd a priori, hence equals 9. On average, they meet $S(\alpha)$ in at least $\frac{8}{9} \mid M \mid$ elements. One easily deduces (see (6), (7) and (8)) that G is of type V.

D. G/N is of type VII. Then G possesses a normal, α-invariant subgroup M of index 2, where M/N has odd order and $s(M/N) = \frac{1}{3}$. Since $S(\alpha) \subset M$ we have $s(M, \alpha) \geq \frac{1}{3}$, which immediately implies that G is of type VII.

E. G/N is of type II. Then G possesses a normal, α-invariant subgroup M such that $G/M \cong A_4$. We proceed to deal with this case in several steps.

Step 1 *:* The number of cosets of M which meet $S(\alpha)$ must be 5.

A priori, this number is either 3 or 5, so suppose it were 3, say $S(\alpha) \subseteq M \cup Mx \cup Mx^{-1}$.

If M is not abelian of odd order, then $\mid M^1 \mid \leq \frac{1}{2} \mid M \mid$, by Theorem A. Since $s(\alpha) \geq \frac{1}{6}$, this forces $\mid M^x \mid \geq \frac{3}{4} \mid M \mid$, and $\mid M_x \mid \geq \frac{1}{2} \mid M \mid$. Since $M_x \subseteq M^1$, the only way to avoid a contradiction is if $s(\alpha) = \frac{1}{6}$ and $s(M, \alpha) = \frac{1}{2}$. Thus M is of type II and G possesses a normal subgroup $Z \subset S(\alpha)$ such that $x \in C_G(Z)$ and G/Z is an extension of C_2 by A_4. Hence $G/Z \cong C_2 \times A_4$ and one easily deduces that G is of type IV, which contradicts the above conclusion that $s(G) = \frac{1}{6}$.

Hence M is abelian of odd order and contained in $S(\alpha)$. Since M^x is now a subgroup of M and $s(G) \geq \frac{1}{6}$, we are forced to conclude that $M^x = M$. In particular, $x \in C_G(M) \lhd G$, implying that $M = Z(G)$. One now easily deduces the contradiction that 5 cosets of M meet $S(\alpha)$. This completes *Step* 1.

Now let us write a coset decomposition

$$G = M \cup Mx \cup Mx^{-1} \cup My \cup My^{-1} \cup Mz_1 \cup \ ... \ \cup Mz_7, \qquad (20)$$

where $\{x, y\} \subset S(\alpha) \subseteq M \cup Mx \cup Mx^{-1} \cup My \cup My^{-1}$. The idea is to look at the groups $A = < M, x >$ and $B = < M, y >$. We have the inequality

$$s(G, \alpha) = s(A, \alpha) + s(B, \alpha) - s(M, \alpha) \geq \frac{1}{6}. \qquad (21)$$

Step 2 *:* Suppose M (and hence A and B) has odd order.

If $M \subset S(\alpha)$ then $s(A, \alpha) > \frac{1}{3}$ so, by the results of [2], $A \subset S(\alpha)$. The same applies to B, and one easily deduces that G is of type II.

If $M \not\subset S(\alpha)$ then [2] implies that $s(A, \alpha)$ and $s(B, \alpha)$ are both $\leq \frac{1}{3}$. But this contradicts (21).

Step 3 *:* Suppose M (and hence A and B) has even order.

For (21) to be satisfied we must have, without loss of generality, that $s(A, \alpha) > \frac{1}{3}$. Applying the induction hypothesis, this implies that $s(A, \alpha) = \frac{5}{12}$ or $\frac{1}{2}$.

Suppose $s(A, \alpha) = \frac{1}{2}$. Thus A possesses an odd-order subgroup $O \subset S(\alpha)$ of index 2. Let $Z = M \cap O$. Evidently, $Z \subseteq Z(G)$ and since G/Z is an extension of C_2 by A_4, we easily conclude that G is of type IV.

Suppose $s(A,\alpha) = \frac{5}{12}$. Then $Z(A)$ has odd order and $A/Z(A) \cong A_4$. Put $Z = Z(A) \cap M$. One easily sees that $Z \subseteq Z(G)$. If $Z = Z(A)$, then G/Z has order 48, being an extension of $C_2 \times C_2$ by A_4. One easily deduces that G is of type V. If $Z \neq Z(A)$, then $M/Z \cong A_4$ and G/Z is an extension of A_4 by A_4, which must be a direct product. One easily deduces that G is of type VI.

F. G/N is of type IV or VI. Similar arguments to those presented already lead one to the conclusion that G is of the same type as G/N. We shall not bother to go into further detail. To finish the proof of Theorem C, there remains to consider

Case II : G possesses no non-trivial, normal, α-invariant subgroup of even index.

By Theorem C, G is soluble. Thus, we must conclude that

(i) G possesses a characteristic, elementary abelian 2-subgroup E with G/E of odd order,

(ii) no proper subgroup of E is G-characteristic.

Since E is a 2-group, $E_x = \{1\}$ for any $x \in S(\alpha)$. Since E is abelian, E^x is a subgroup of E. Since $s(G) \geq \frac{1}{6}$, there is some $x \in S(\alpha)$ such that $\mid E^x \mid \geq \frac{1}{6} \mid E \mid$. By (6) this implies that $\sqrt{\mid E \mid} \geq \frac{1}{6} \mid E \mid$. Hence, $\mid E \mid = 2, 4, 8, 16$ or 32. At this stage, one looks at the natural map from $G/E \rightarrow \mathrm{Aut}(E)$.

If $\mid E \mid = 2$, then E is obviously a direct factor of G and G is of type I or VII as in the theorem.

E cannot have order 8 or 32, because condition (ii) cannot be satisfied.

If $\mid E \mid = 4$, then for (ii) to be satisfied, G must possess a central, odd-order subgroup N with $G/N \cong A_4$. Since we are in Case II, $N = \{1\}$ and G is minimal of type II. Similarly, if $\mid E \mid = 16$, one sees that G must be minimal of type V.

We have thereby completed the proof of Theorem B, part (i).

4. Proof of Theorem B, part (ii) : Explicit automorphisms. We conclude by giving, for each group G of types I through VI in Theorem B, a description of an automorphism α of G such that $s(\alpha) = s(G) > \frac{1}{6}$.

Type I : Let A be the odd order abelian subgroup of index 2 and x any element of order 2 in G. Then the map

$$\alpha(x) = x, \qquad \alpha(a) = a^2 \; \forall \; a \in A,$$

extends to an automorphism of G and satisfies $s(\alpha) = s(G) = \frac{1}{2}$.

Type II : Let β be the automorphism of $Z(G)$ which squares every element. Let γ be the automorphism of $G/Z(G) \cong A_4$ induced by conjugation by a transposition in S_4. It was proven in [8] that there exists an automorphism α of G inducing β and γ, and that $s(\alpha) = s(G) = \frac{5}{12}$.

Type III : Let A be the odd order normal subgroup of index 4, and let X be any complement of order 4. The map

$$\alpha(x) = x \; \forall \; x \in X, \qquad \alpha(a) = a^2 \; \forall \; a \in A,$$

extends to an automorphism of G and satisfies $s(\alpha) = s(G) = \frac{1}{4}$.

Type IV : The group $G/Z(G)$ is a split extension of A_4 by C_2. Since $\mathrm{Inn}(A_4) \cong S_4$, we see easily that either $G/Z(G) \cong A_4 \times C_2$ or $G/Z(G) \cong S_4$.

In the first case, $G = H \times C_2$ where H is a group of Type II. Then the map $\alpha = \alpha_1 \times \mathrm{id}$, where α_1 is an automorphism of H with $s(H, \alpha_1) = \frac{5}{12}$, is an automorphism of G satisfying $s(\alpha) = s(G) = \frac{5}{24}$.

In the second case, the Universal Coefficients Theorem implies that the extension must be split, hence a direct product, i.e.: $G = Z(G) \times K$, where $K \cong S_4$. Let β be conjugation by a transposition in S_4. Then $s(S_4, \beta) = \frac{5}{24}$ and the map $\alpha : G \to G$ given by

$$\alpha(zk) = z^2 \beta(k)$$

is an automorphism of G with $s(\alpha) = s(G) = \frac{5}{24}$,

Type V : Let β be the automorphism of Z which squares every element. We shall construct an automorphism γ of $G/Z \cong H$ such that

(i) $s(H, \gamma) = \frac{9}{48}$,

(ii) there exists an automorphism α of G inducing β and γ, such that $s(G, \alpha) = s(G) = \frac{9}{48}$.

Write $H = E \times C$ where E is elementary abelian of order 16, C is of order

3, and C acts fixed-point freely on E. Since $\mathrm{ord}_3|GL(4,\mathbf{F}_2)| = 2$, there is no loss of generality in presenting H as follows :

$$\begin{array}{rr} E = <a> \times <b> \times <c> \times <d>, \\ C = <e>, \\ e^{-1}ae = b \quad e^{-1}ce = d \\ e^{-1}be = ab \quad e^{-1}de = cd. \end{array}$$

Then one may check that the map

$$\gamma(a) = b, \quad \gamma(b) = a, \quad \gamma(c) = d, \quad \gamma(d) = c, \quad \gamma(e) = e^2,$$

extends to an automorphism of H for which $s(\gamma) = \frac{9}{48}$.

The proof of (ii) employs the Filling Lemma in exactly the same way as in [8]. We refer to that paper for details.

TYPE VI : It is easy (if a little tedious) to check that an automorphism γ of $A_4 \times A_4$ squares 25 elements if and only if $\gamma = \gamma_1 \times \gamma_2$, where each γ_i is an automorphism of one of the factors which squares 5 elements, and hence is induced by conjugation by an involution in S_4.

Pick any such automorphism γ, and let β the automorphism of Z which squares every element. Then, by the same argument as in [8], there exists an automorphism of G inducing β and γ, and clearly $s(\alpha) = s(G) = \frac{25}{144}$.

Acknowledgement. I wish to thank the referee for very helpful suggestions regarding the presentation of the paper.

References

[1] J.H. CONWAY, R.T. CURTIS, S.P. NORTON, R.A. PARKER and R.A. WILSON, Atlas of Finite Groups. Clarendon Press, Oxford, 1985.

[2] H. LIEBECK, Groups with an automorphism squaring many elements. J. Austral. Math. Soc. **16**, 33-42 (1973).

[3] H. LIEBECK and D. MACHALE, Groups with automorphisms inverting most elements. Math. Z. **124**, 51-63 (1972).

[4] H. LIEBECK and D. MACHALE, Groups of odd order with automorphisms inverting many elements. J. Lond. Math. Soc. (2) **6**, 215-223 (1973).

[5] W.M. Potter, Nonsolvable groups with an automorphism inverting many elements. Arch. Math. **50**, 292-299 (1988).
[6] W.R. Scott, Group Theory. Dover, New York, 1964.
[7] M. Suzuki, Group Theory, Vol. I. Springer-Verlag, New York, 1982.
[8] J. Zimmerman, Groups with automorphisms squaring most elements. Arch. Math. **54**, 241-246 (1990).

Anschrift des Autors :

P.V. Hegarty
Department of Mathematics
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg
Sweden
hegarty@math.chalmers.se