BULL. AUSTRAL. MATH. SOC. 20D99, 20D10
VOL. 44 (1991) [429–450]

SMALL SQUARING AND CUBING PROPERTIES FOR FINITE GROUPS

YA. G. BERKOVICH, G.A. FREIMAN AND CHERYL E. PRAEGER

A group G is said to have the small squaring property on k-sets if $\left|K^2\right| < k^2$ for all k-element subsets K of G, and is said to have the small cubing property on k-sets if $\left|K^3\right| < k^3$ for all k-element subsets K. It is shown that a finite nonabelian group with the small squaring property on 3-sets is either a 2-group or is of the form TP with T a normal abelian odd order subgroup and P a nontrivial 2-group such that $Q = C_P(T)$ has index 2 in P and P inverts T. Moreover either P is abelian and Q is elementary abelian, or Q is abelian and each element of $P - Q$ inverts Q. Conversely each group of the form TP as above has the small squaring property on 3-sets. As for the nonabelian 2-groups with the small squaring property on 3-sets, those of exponent greater then 4 are classified and the examples are similar to dihedral or generalised quaternion groups. The remaining classification problem of exponent 4 nonabelian examples is not complete, but these examples are shown to have derived length 2, centre of exponent at most 4, and derived quotient of exponent at most 4. Further it is shown that a nonabelian group G satisfies $\left|K^2\right| < 7$ for all 3-element subsets K if and only if $G = S_3$. Also groups with the small cubing property on 2-sets are investigated.

1. INTRODUCTION

The problems considered in this paper come from a class of problems suggested by the second author, namely problems concerning the size of $K^m = \{a_1a_2\dots a_m \mid a_i \in K \text{ for } 1 \leqslant i \leqslant m\}$ for a k-element subset K of a group G as a function of k and m. Several problems of this type have been considered in the literature. For example if G is the additive group of integers and K is a set of k integers then (writing $K + K$ for K^2)

$$2k - 1 \leqslant |K + K| \leqslant k(k+1)/2$$

and it was shown in [7], see also [10], that $|K + K| = 2k - 1$ if and only if K is an arithmetic progression. Also, in [7], the structure of K was determined if $|K + K| < ck$ for some constant c and k sufficiently large. More generally if G is any torsion free

Received 3 December 1990
We wish to thank George Glauberman for suggesting a simplification of the proof of Lemma 5.4 (which is used to prove Theorem 5.1).

group then (see [14], [10, Theorem 3] and [5]), $|K^2| \geqslant 2k-1$ and equality holds if and only if K is a progression, that is $K = \{a, ac, \ldots, ac^{k-1}\} = \{b, db, \ldots, d^{k-1}b\}$ for some $a, b, c, d \in G$ with $c \neq 1$, $d \neq 1$. On the other hand if G is not torsion free then it is possible for $|K^2|$ to be less than $2k-1$. Trivially if G is a finite group and $K = G$ then $K^2 = K$. In [8] the second author showed that $|K^2| < 3|K|/2$ for some finite subset K of a group G if and only if either $K^2 = \langle K \rangle$ (the group generated by K) or $K \subseteq gN$ for some $g \in G$ and some normal subgroup N of G of order $|K^2|$.

Let us say that a group G has the *small squaring property* on k-sets if $|K^2| < k^2$ for all k-element subsets K. In order to gain an understanding of the structural restrictions placed on a group by the small squaring property on k-sets for a fixed k, the second author ([9]; see also [4]) investigated this property for 2-element subsets and showed that a finite group has the small squaring property on 2-sets if and only if it is a Dedekind group, that is, either it is abelian or the direct product of an elementary abelian 2-group and the quaternion group Q_8 of order 8. Recently Neumann [17] has shown that a group G has the small squaring property on k-sets if and only if G has normal subgroups M, N with $1 \leqslant M < N \leqslant G$ such that $|M|$ and $|G/N|$ are bounded above by a function of k, and N/M is abelian, that is G is "finite by abelian by finite". In the present paper we consider finite groups with the small squaring property on 3-sets and obtain an almost complete characterisation, namely we obtain a characterisation of all examples except those of exponent 4. The first main result is the following theorem which is proved in Section 2.

Theorem 1. *Let G be a finite group such that $|K^2| < 9$ for all 3-element subsets K of G. Then one of the following is true.*

(a) *The group G is abelian.*
(b) *The group G is a nonabelian 2-group.*
(c) *The group $G = TP$ where T is a nontrivial normal abelian odd order subgroup and P is a nontrivial 2-group. Further the subgroup Q of P which centralises T has index 2 in P and each element of $P - Q$ inverts T, and either*
    (i) *P is abelian and Q is elementary abelian, or*
    (ii) *P is nonabelian, Q is abelian, and each element of $P-Q$ inverts Q.*

Conversely any group satisfying (a) or (c) has the small squaring property on 3-sets.

In Section 3 nonabelian 2-groups with the small squaring property on 3-sets are investigated. They are shown (Theorem 2) to be similar to dihedral or generalised quaternion groups unless they have exponent 4, derived length 2, and a very restrictive structure on the centre and derived quotient. We obtain a complete characterisation of all examples of exponent at least 8.

If we impose an even stronger restriction on the orders of the squares of 3-element subsets then we obtain the following result. It will be proved in Section 4.

THEOREM 3. *Let G be a finite nonabelian group. Then G has the property that $|K^2| < 7$ for all 3-element subsets K of G if and only if $G = S_3$.*

In Section 5 we consider finite groups with the small cubing property on 2-sets. Our main result, Theorem 5.1, is fairly technical but is sufficiently strong to characterise all odd order examples:

THEOREM 4. *Let G be a group of odd order. Then $|K^3| < 8$ for all 2-element subsets K of G if and only if either G is abelian or G is a nonabelian group of exponent 3.*

This problem was first considered in an unpublished manuscript [**3**] of the first two authors where a weak version of Theorem 5.1 was proved. The version of Theorem 5.1 in [**3**] was improved in [**6**, Theorem 3] to give a characterisation of all examples of finite groups G with the small cubing property on 2-sets except for the case where G has a normal abelian 2-complement. Their result [**6**, Theorem 3] is rather technical for use in applications. We derive from our result, Theorem 5.1, the following characterisation of finite groups G in which $|K^3| < 6$ for all 2-element subsets K of G.

THEOREM 5. *Let G be a finite group. Then $|K^3| < 6$ for all 2-element subsets K of G if and only if either G is abelian or G is a nonabelian 2-group satisfying one of*

(a) *$G = \langle a, H\rangle$ where H is an abelian subgroup of index 2 in G and of exponent 4, and a has order 2 and inverts H.*

(b) *The Frattini subgroup $\Phi(G)$ of G has order 2.*

2. NONABELIAN GROUPS OTHER THAN 2-GROUPS WITH SMALL SQUARING ON 3-SETS

Suppose that G is a finite nonabelian group which is not a 2-group and which has the small squaring property on 3-sets. We shall show that G satisfies part (c) of Theorem 1. Note that each subgroup and quotient group of G has the small squaring property on 3-sets. First we consider odd ordered Sylow subgroups of G.

LEMMA 2.1. *Each Sylow subgroup of G of odd order is abelian.*

PROOF: Suppose that P is a nonabelian p-subgroup of G for some odd prime p. Then $P/Z(P)$, where $Z(P)$ is the centre of P, is not cyclic and so P has distinct maximal subgroups M and N containing $Z(P)$ (see [**12**, 5.1]). Further M and N are normal subgroups of P. Let $Q = M \cap N$ and let $a \in M - Q$. Now M and N are generated by $M - Q$ and $N - Q$ respectively. Thus $\langle a, N - Q\rangle = \langle a, N\rangle = P$, so if a centralised every element of $N - Q$ then a would lie in the centre of P which is not the case. So there is an element $b \in N - Q$ such that $ab \neq ba$. Let $K = \{a, ab, b^2\}$. Then $|K| = 3$ and we claim that $K^2 = \{a^2, a^2b, ab^2, aba, abab, ab^3, b^2a, b^2ab, b^4\}$ has order 9.

Note that since M is normal in P, the coset of M containing the word $w = a^{i_1}b^{j_1}\dots a^{i_r}b^{j_r}$ is the coset b^jM where $j = \sum j_k$ and the coset of N containing w is a^iN where $i = \sum i_k$.

So, for example, the only elements of K^2 in M are a^2, ab^3 and b^2ab, the latter two lying in M if and only if $b^3 \in M$. Then as a^2N is different from the coset of N containing ab^3 or b^2ab it follows that a^2 is not equal to any of the other words in K^2. Similarly, considering membership of N we find that b^4 is not equal to any of the other words in K^2. Also the only elements of K^2 in $a^2N - M$ are a^2b, aba, and $abab$ and clearly these are all distinct. Thus the only equalities among the expressions in K^2 must be between ab^2, b^2a, ab^3 and b^2ab. The first two of these lie in b^2M and the last two are in b^3M so the only possible equalities are $ab^2 = b^2a$ and $ab^3 = b^2ab$, each of which implies the other. However as b has odd order $ab^2 = b^2a$ is equivalent to $ab = ba$ which does not hold. Thus $|K^2| = 9$ which is a contradiction. ∎

Lemma 2.2. *A finite group of odd order with the small squaring property on 3-sets is abelian.*

Proof: Suppose that there is a finite nonabelian group of odd order with the small squaring property on 3-sets and let G be such a group with the least possible order. Then all proper subgroups of G are abelian. By Lemma 2.1 it follows that G is not nilpotent and so by a result of Schmidt, see [**18**, 9.1.9] or [**11**], $|G| = p^uq^v$ where p and q are distinct primes and G has a cyclic Sylow p-subgroup $P = \langle a\rangle$ which is not normal in G and a normal Sylow q-subgroup Q. Since G is nonabelian a does not centralise Q, that is $ab \neq ba$ for some $b \in Q$. Suppose first that $|P| = p^u > 3$ and let $K = \{b, a, ba^2\}$. We claim that $K^2 = \{b^2, b^2a^2, ba, ba^2b, ba^3, ba^2ba^2, a^2, ab, aba^2\}$ has order 9. As in the previous lemma $a^{i_1}b^{j_1}\dots a^{i_r}b^{j_r}Q = a^iQ$ where $i = \sum i_k$. Thus the only element of $K^2 \cap Q$ is b^2, the only elements of K^2 in aQ are ab and ba and these are distinct, the only elements of K^2 in a^3Q are ba^3 and aba^2 and these are distinct, and the only element of K^2 in a^4Q is ba^2ba^2. Thus the only possible equalities among the expressions in K^2 are between b^2a^2, ba^2b and a^2 and here the possibilities are $b^2a^2 = ba^2b$ or $ba^2b = a^2$. The former is equivalent to $ba^2 = a^2b$ which implies $ba = ab$ (since a has odd order) and so does not hold. The latter is equivalent to $a^{-2}ba^2 = b^{-1}$ which implies $ba^4 = a^4b$ and hence $ba = ab$, which again is not true. Thus $|K^2| = 9$ which is a contradiction.

Thus $|P| = p^u = 3$. In this case let $K = \{a, b, ab\}$ so that

$$K^2 = \{a^2, a^2b, ab, aba, ab^2, abab, ba, b^2, bab\}.$$

Again the only element of K^2 in Q is b^2. The elements of K^2 in aQ are ab, ab^2, ba and bab and the only possible equality among these is $ab^2 = ba$, that is $a^{-1}ba = b^2$, so that $b = a^{-3}ba^3 = b^8$, that is $b^7 = 1$. In this case $\langle a, b\rangle$ is a nonabelian subgroup of G of order 21 and hence $G = \langle a, b\rangle$, but it is easy to check that $|L^2| = 9$ for $L = \{a, b^2, ab\}$ which is a contradiction. Thus ab, ab^2, ba and bab are all distinct, and the only equalities among expressions in K^2 must be between the elements a^2, a^2b, aba and $abab$ of $K^2 \cap a^2Q$. Here the only possibility is $a^2 = abab$, that is $a^{-1}ba = b^{-1}$ which implies $ba^2 = a^2b$ and hence $ba = ab$ which is not the case. This final contradiction completes the proof $\square$

Now let P be a Sylow 2-subgroup of G. We show next that G has a normal 2-complement.

Lemma 2.3. *The group G has a normal subgroup T of odd order such that $G = TP$.*

Proof: Suppose that there is a finite nonabelian group with the small squaring property on 3-sets which does not have a normal odd order subgroup of 2-power index, and let G be such a group with minimum order. Then every proper subgroup of G has an odd order normal subgroup of 2-power index and so by [**13**, IV.5.4], the Sylow 2-subgroup P is normal in G of exponent at most 4, $|G/P| = q^v$ for some odd prime q and a Sylow q-subgroup Q of G is cyclic, say $Q = \langle a\rangle$. Since Q is not normal in G, there is an element $b \in P$ such that $ab \neq ba$. Let $K = \{a, b, ab\}$. We claim that $|K^2| = 9$ contradicting the small squaring property of G. Now $K^2 \cap aP = \{ab, ba, bab, ab^2\}$ and the only possible equality among these expressions is $ba = ab^2$, that is, $a^{-1}ba = b^2$. This implies that b and b^2 have the same order which is not true. Also, $K^2 \cap a^2P = \{a^2, a^2b, aba, abab\}$ and the only possible equality among these expressions is $a^2 = abab$, that is $a^{-1}ba = b^{-1}$ so that b commutes with a^2 and hence with a which is not the case. Thus $|K^2| = 9$ and this contradiction completes the proof. $\square$

Lemma 2.4. *The normal subgroup T is abelian and is not centralised by P.*

Proof: It follows from Lemma 2.2 that T is abelian. Suppose that P centralises T. Then $G = P \times T$ and as G is not abelian, P is not abelian. As in the proof of Lemma 2.1, P has distinct maximal normal subgroups M and N containing $Z(P)$ and there are elements $a \in M - N$ and $b \in N - M$ such that $ab \neq ba$. Let $c \in T - \{1\}$ and consider $K = \{a, bc, abc^2\}$. (Note that c commutes with a and b and, if $w = a^{i_1}b^{j_1}\dots a^{i_r}b^{j_r}$ then $wM = b^jM$, $wN = a^iN$ where $j = \sum j_k$, $i = \sum i_k$.) Then $K^2 \cap (N \times T) =$

$\{b^2c^2\}$, $K^2 \cap a(N \times T) = \{abc, bac, ab^2c^3, babc^3\}$ and these elements are all distinct since $ab \neq ba$ and c has odd order, $K^2 \cap a^2(N \times T) = \{a^2bc^2, abac^2, a^2, ababc^4\}$ and again these elements are all distinct. Thus $|K^2| = 9$ which is a contradiction. ∎

LEMMA 2.5. *The subgroup P has a subgroup Q of index 2 which centralises T and every element of $P - Q$ inverts T.*

PROOF: Let $a \in P$ be an element which does not centralise T, so $ab \neq ba$ for some $b \in T$. First we show that $a^2b = ba^2$. This is true if $a^2 = 1$ so assume that $a^2 \neq 1$ and consider $K = \{b, ba, ba^2\}$. Then $K^2 \cap aT = \{b^2a, bab\}$ has order 2, $K^2 \cap a^3T = \{baba^2, ba^2ba\}$ has order 2, and $K^2 \cap (T \cup a^4T) = \{b^2, ba^2ba^2\}$, $K^2 \cap a^2T = \{b^2a^2, baba, ba^2b\}$. Since $|K^2| < 9$ some pair of expressions in one of the latter two sets must be equal in G. The only possibilities are $b^2 = ba^2ba^2$ with $a^4 = 1$, or $b^2a^2 = ba^2b$. In either case $ba^2 = a^2b$.

Now consider $K = \{b, ba, b^2a\}$. We have $K^2 \cap aT = \{b^2a, b^3a, bab, b^2ab\}$ and $K^2 \cap (T \cup a^2T) = \{b^2, baba, bab^2a, b^2aba, b^2ab^2a\}$. Since $|K^2| < 9$ some pair of expressions in one of these sets must be equal in G. If $a^2 \neq 1$ then the only possibilities are $b^3a = bab$ and $baba = b^2ab^2a$. The latter is equivalent to $a^{-1}ba = b^{-1}$. In the case of the former equality we have $aba^{-1} = b^2$, and as $ba^2 = a^2b$ we have $b = a^2ba^{-2} = b^4$. Thus $b^3 = 1$ and so $aba^{-1} = b^{-1}$. In either case a inverts b. If $a^2 = 1$ then apart from the above possibilities there is also the possible equality $b^2 = bab^2a$. This implies that $aba = b^2$ and hence that $b = a^2ba^2 = b^4$ whence $b^3 = 1$. Thus in all cases a inverts b.

Thus, for each $x \in T$, $x^a = a^{-1}xa$ is either x or x^{-1}, and for some $b \in T - \{1\}$, $b^a = b^{-1}$. Suppose there is an $x \in T = \{1\}$ which commutes with a. Then $(xb)^a = xb^{-1}$ is either xb or $(xb)^{-1} = x^{-1}b^{-1}$ (since T is abelian). Neither of these is possible and hence a inverts each element of T.

Thus each element of P either centralises or inverts T and so P has a subgroup Q of index 2 which centralises T. ∎

At this point we distinguish two cases according as P is abelian or not.

LEMMA 2.6. *Either P is abelian or there are elements $a \in P - Q$ and $b \in Q$ such that $ab \neq ba$.*

PROOF: If $a \in P - Q$ centralises Q then a centralises $\langle a, Q\rangle = P$, that is $a \in Z(P)$. Thus if each element of $P - Q$ centralised Q then each element of $\langle P - Q\rangle = P$ would centralise Q and hence would lie in $Z(P)$, that is P would be abelian. ∎

First we consider the case of P abelian.

LEMMA 2.7. *(a) If P is abelian then Q is elementary abelian.*

(b) Conversely suppose that $G = TP$ is a finite group with T a nontrivial abelian odd order normal subgroup and P an abelian 2-group such that the centraliser $Q =$

$C_P(T)$ of T in P is elementary abelian of index 2 in P and P inverts T. Then G has the small squaring property on 3-sets.

PROOF: (a) Suppose that P is abelian and that Q contains an element b of order 4. Let $a \in P - Q$. By replacing b by b^{-1} if necessary we may assume that $a^2b \neq 1$. Let $c \in T - \{1\}$ and consider $K = \{ac, abc^2, c\}$. (Recall that $bc = cb$ and $ac = c^{-1}a$.) Now $K^2 \cap P$ consists of $(ac)^2 = a^2$, $cac = a$, $(abc^2)^2 = a^2b^2$, and also $abc^3 = ab$ if $c^3 = 1$, and these elements are all distinct. The elements of K^2 not in $T \times Q$ are ac^2, a, abc^3, and $c(abc^2) = abc$ and these are all distinct. The elements of $K^2 \cap (T \times Q)$ not in P are $ac(abc^2) = a^2bc$, $abc^2(ac) = a^2bc^{-1}$, and c^2 and these are all distinct. Thus $|K^2| = 9$ which is a contradiction. So Q is elementary abelian.

(b) Let G, T, P, Q be as stated and let $a \in P - Q$. Let K be any 3-element subset of G. If K contains at least two elements of $T \times Q$ then $|K^2| < 9$ since $T \times Q$ is abelian. So assume that K contains two elements of $G - (T \times Q)$ say $x = abc$ and $x' = ab'c'$ where b, $b' \in Q$ and c, $c' \in T$. Then $x^2 = (abc)^2 = a^2$ since $ca = ac^{-1}$, and $b^2 = 1$, similarly $(x')^2 = a^2$. Thus $|K^2| < 9$ and so G has the small squaring property on 3-sets. ∎

Now we consider the case where P is not abelian.

LEMMA 2.8. *If P is not abelian then Q is abelian and each element of $P - Q$ inverts Q.*

PROOF: By Lemma 2.6 there are elements $a \in P - Q$ and $b \in Q$ such that $ab \neq ba$. Consider $K = \{a, ab, c\}$ where $c \in T - \{1\}$. The elements of K^2 not in $T \cup P$ are ac, ca, abc, cab and these are all distinct. The elements of $K^2 \cap P$ are a^2, a^2b, aba and $abab$. Since $|K^2| < 9$ at least two of these elements are equal and hence $a^2 = abab$, that is $b^a = b^{-1}$. In particular $b^2 \neq 1$. Thus a centralises or inverts each element of Q. If a inverts each element of Q then, for x, $y \in Q$, $x^{-1}y^{-1} = (yx)^{-1} = (yx)^a = y^a x^a = y^{-1}x^{-1}$ and it follows that Q is abelian. Also in this case each element of $P - Q$ is of the form ax for some $x \in Q$, and ax inverts Q. Thus we may assume that, for some $c \in Q$, $c^a = c \neq c^{-1}$. In particular $c \neq b$, $c \neq b^{-1}$ and $c^2 \neq 1$. Now $(bc)^a = b^a c^a = b^{-1}c \neq bc$ and hence $(bc)^a = (bc)^{-1}$. It follows that $bc = (b^{-1}c)^{-1}$, that is b inverts c. (In particular $bc \neq cb$.)

Now consider $K = \{a, bx, cy\}$ where x, y are distinct nontrivial elements of T. The elements of K^2 not in $T \times Q$ are abx, acy, $bxa = ab^{-1}x^{-1}$, $cya = acy^{-1}$ and these are all distinct. The elements of K^2 in $T \times Q$ are a^2, b^2x^2, c^2y^2, $bcxy$, $cbxy$ and as $|K^2| < 9$ at least two of these elements are equal. It follows that $xy = 1$ and either $a^2 = bc$ or $a^2 = cb$. It follows that c (equal to $b^{-1}a^2$ or a^2b^{-1}) commutes with b. This contradiction completes the proof. ∎

LEMMA 2.9. *Let $G = TP$ be a finite group with T a nontrivial abelian odd* *order normal subgroup and P a 2-group such that the centraliser $Q = C_P(T)$ of T in P is abelian of index 2 in P and P inverts $T \times Q$. Then G has the small squaring property on 3-sets.*

PROOF: Let K be a subset of G of order 3. If K contains at least two elements of the abelian group $T \times Q$ then $|K^2| < 9$. So assume that K contains two elements not in $T \times Q$, say $x = abc$ and $x' = ab'c'$ where $a \in P - Q$, $b, b' \in Q$, $c, c' \in T$. Then $x^2 = a^2 = (x')^2$ and hence again $|K^2| < 9$. ∎

3. Nonabelian 2-groups with the small squaring property on 3-sets

Here we investigate nonabelian 2-groups with the small squaring property on 3-sets. A complete classification is obtained of those with exponent at least 8. First let us consider some examples.

DEFINITION 3.1: (a) A 2-group G is called a *D-group* if it is nonabelian and the subgroup $A = \langle x \mid x \in G, x^2 \neq 1\rangle$ is a proper subgroup of G.

(b) A 2-group G is called a *Q-group* if it is nonabelian and satisfies the following conditions.

- (i) G has a subgroup A of index 2 such that each element of $G - A$ has order 4.
- (ii) If $x, y \in G - A$ then $x^2 = y^2$ and $a^x = x^{-1}ax = a^{-1}$ for all $a \in A$.

The dihedral and generalised quaternion groups of order $2^n \geqslant 8$ are examples of D-groups and Q-groups respectively. All D-groups and Q-groups have the small squaring property on 3-sets.

LEMMA 3.2. *(a) If a 2-group G is a D-group then $A = \langle x \mid x^2 \neq 1\rangle$ is an abelian subgroup of index 2, each element of $G - A$ inverts A, and G has the small squaring property on 3-sets.*

(b) If a 2-group G is a Q-group then G has the small squaring property on 3-sets and the subgroup A of 3.1 (b)(i) is abelian.

PROOF: (a) Since $G = \langle G - A\rangle$ and G is nonabelian there are non-commuting elements x, y in $G - A$ and by the definition of A, $x^2 = y^2 = 1$. Suppose that $|G : A| > 2$. Then we may choose x and y so that $xy \neq yx$ and also $xA \neq yA$. Since A is normal in G, the four cosets A, xA, yA and $xyA = Axy$ are all distinct. Thus $xy \in G - A$ and hence has order 2. This implies that $xy = yx$ which is a contradiction. Thus A has index 2 in G. Now if $a \in A$ then $xa \in G - A$ and so $(xa)^2 = 1$, that is $a^x = a^{-1}$. So x inverts every element of A and it follows that A is abelian. Let K be a 3-element subset of G. If $|K \cap A| \geqslant 2$ then $|K^2| < 9$ since A is abelian while if K contains two elements x, y of $G - A$ then $x^2 = y^2 = 1$ and again $|K^2| < 9$.

(b) Since an element of $G - A$ inverts A, A is abelian. Then if K is a 3-element subset of G, $|K^2| < 9$ when $|K \cap A| \geqslant 2$ since A is abelian, and $|K^2| < 9$ when K contains two elements x, y of $G - A$ since $x^2 = y^2$. ∎

The main result which will be proved in this section is the following theorem.

Theorem 2. *Let G be a nonabelian 2-group such that $|K^2| < 9$ for all 3-element subsets K of G. Then either*

(a) *G is a D-group or a Q-group, or*

(b) *G has exponent 4 and derived length 2. Further each of the centre $Z(G)$ and the derived quotient G/G' is either elementary abelian or the product of an elementary abelian group and a cyclic group of order 4.*

Conversely each 2-group which is a D-group or a Q-group has the small squaring property on 3-sets.

The problem of determining all exponent 4 examples is open. There are certainly examples which are not D-groups or Q-groups and this is demonstrated in the following result.

Proposition 3.3. *Let G be a nonabelian 2-group which is minimal (by inclusion) such that $|K^2| < 9$ for all 3-element subsets K. Then G is D_8, Q_8 or $T = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^{-1}\rangle$ (and all of these groups have the small squaring property on 3-sets).*

Proof: If $|G| = 8$ then G is D_8 or Q_8 which have the small squaring property by Lemma 3.2, so assume that $|G| \geqslant 16$. Now G is a minimal nonabelian 2-group since all subgroups of G have the small squaring property. Then, see [**13**, p.309], either

$$G = G_1 = \langle a, b \mid a^{2^\alpha} = b^{2^\beta} = 1, b^{-1}ab = a^{1+2^{\alpha-1}}\rangle$$

with $\alpha \geqslant 2$, and $|G| = 2^{\alpha+\beta}$, or

$$G = G_2 = \langle a, b \mid a^{2^\alpha} = b^{2^\beta} = 1, [a, b]^2 = 1\rangle,$$

with say $\alpha \geqslant 2$ and $|G| = 2^{\alpha+\beta+1}$.

Suppose $G = G_1$. Then $Z(G) = \langle a^2, b^2\rangle$ has index 4. If $\alpha = 3$ then $|K^2| = 9$ for $K = \{a, b, ba\}$, so $\alpha = 2$ and hence $\beta \geqslant 2$. If $\beta \geqslant 3$ then $|K^2| = 9$ for $K = \{a, b, ab^3\}$, so $\beta = 2$ and $G = T$. It can be checked that T has the small squaring property on 3-sets.

Now let $G = G_2$. Then $Z(G) = \langle a^2, b^2, [a, b]\rangle$ again has index 4, and $|K^2| = 9$ if $K = \{a, b, ba\}$. Thus G_2 does not have the small squaring condition. ∎

This result is very important when investigating nonabelian 2-groups G with the small squaring property on 3-sets as the small squaring property is inherited by subgroups and quotient groups. For example if H is a minimal nonabelian subgroup of

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

G, then by Proposition 3.3, H is isomorphic to D_8, Q_8, or the group T defined there. Also if A is a cyclic subgroup of $Z(G)$ then HA is a direct product or a central product of H and A, and HA has the small squaring property on 3-sets. We shall need some information about such products.

PROPOSITION 3.4. *(a) None of the central products $Z_8 * D_8$ and $Z_8 * Q_8$ and the direct product $Z_8 \times Q_8$ has the small squaring property on 3-sets.*

(b) The direct product $Z_4 \times L$ of a cyclic group of order 4 and a nonabelian 2-group L has the small squaring property on 3-sets if and only if $L = Q_8 \times E$, where E is an elementary abelian 2-group or $E = 1$.

(c) A central product of a cyclic group $Z_4 = \langle c \rangle$ and the group $T = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^{-1} \rangle$ has the small squaring property on 3-sets if and only if $c^2 = a^2 b^2$. A central product of the abelian group $Z_4 \times Z_4 = \langle c \rangle \times \langle d \rangle$ and T does not have the small squaring property on 3-sets.

PROOF: (a) This is proved by showing that $|K^2| = 9$ for the following sets K. For $Z_8 * D_8 = \langle c, a, b \mid a^4 = b^2 = 1, c^4 = a^2, ca = ac, cb = bc, ba = a^3 b \rangle$ let $K\{a, b, abc\}$, and for $Z_8 \times Q_8 = \langle c \rangle \times \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3 b \rangle$ and $Z_8 * Q_8 = \langle c, a, b \mid a^4 = 1, c^4 = a^2 = b^2, ca = ac, cb = bc, ba = a^3 b \rangle$ let $K = \{a, bc, abc^3\}$.

(b) Suppose that $Z_4 \times L = \langle c \rangle \times L$ has the small squaring property on 3-sets but that L is not of the required form. Then by Freiman [9], there is a subset $K_0 = \{a, b\}$ of L such that $|K_0^2| = 4$. Since for $K = \{a, b, abc\}$ we must have $|K^2| < 9$, it follows that $b(abc) = (abc)a$ and hence that $a = (ab)^{-1} b(ab)$. Thus $L_0 = \langle a, b \rangle$ is a finite nonabelian 2-group in which a and b are conjugate. This is impossible. (For suppose that $L_0 = \langle a, b \rangle$ has least order among finite nonabelian 2-groups with the generators a and b conjugate in L_0. Then $L_0/Z(L_0) = \langle aZ(L_0), bZ(L_0) \rangle$ has its generators $aZ(L_0)$ and $bZ(L_0)$ conjugate, so by minimality $L_0/Z(L_0)$ is abelian. As $aZ(L_0)$ and $bZ(L_0)$ are conjugate in $L_0/Z(L_0)$ they are equal and hence $L_0/z(L_0)$ is cyclic. Thus L_0 is abelian, which is a contradiction.) Thus L is of the required form.

Conversely consider $H = Z_4 \times L = \langle c \rangle \times L$ where $L = Q \times E$, with $Q = \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3 b \rangle$ and E an elementary abelian 2-group. Let K be a 3-element subset of H. If $K \cap L$ contains distinct elements x and x' then by [9], $|\{x, x'\}^2| < 4$ and so $|K^2| < 9$. Similarly if $K \cap (cL \cup c^3 L)$ contains distinct elements $c^\delta x$ and $c^{\delta'} x'$, where $\delta, \delta' \in \{1, 3\}$ and $x, x' \in L$, then $\{c^\delta x, c^{\delta'} x'\}^2 = c^2 \{x, x'\}^2$ has size at most 3 and so $|K^2| < 9$. Again if $K \cap c^2 L$ contains distinct elements $c^2 x$ and $c^2 x'$, where $x, x' \in L$ then $\{c^2 x, c^2 x'\}^2 = \{x, x'\}^2$ has size at most 3 and $|K^2| < 9$. The remaining case to be considered is $K = \{x, c^2 x', c^\delta x''\}$ where $x, x', x'' \in L$ and δ is 1 or 3. If any one of x, x', x'' lies in $Z(L)$ then $|K^2| < 9$. So we may assume that all of them lie in $L - Z(L)$, but then $x^2 = x'^2$ and again $|K^2| < 9$. Thus H has the small

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

squaring property on 3-sets.

(c) By (b), $T \cap \langle c \rangle \neq 1$. Hence $c^2 \in \{a^2, b^2, a^2b^2\}$. Take $K = \{a, b, abc\}$. If $|K^2| < 9$ then $c^2 \neq a^2, b^2$. Thus $c^2 = a^2b^2$, and in this case it is easy to check that $T * \langle c \rangle$ with $c^2 = a^2b^2$ has the small squaring property on 3-sets. Finally suppose that some central product $G = T * (\langle c \rangle \times \langle d \rangle)$ has the small squaring property. Then $T * \langle c \rangle$ and $T * \langle d \rangle$ have the small squaring property also, and hence $c^2 = a^2b^2 = d^2$. Therefore $c^2 = d^2 \in \langle c \rangle \cap \langle d \rangle$, which is a contradiction. ∎

This Proposition yields the result claimed for the structure of $Z(G)$ in Theorem 3.

Theorem 3.5. *Let G be a nonabelian 2-group with the small squaring property on 3-sets. Then $Z(G)$ is either E or $E \times Z_4$, where E is elementary abelian (or trivial).*

Proof: Let H be a minimal nonabelian subgroup of G. Suppose that $Z(G)$ is not elementary abelian and let $A = \langle a \rangle$ be a cyclic direct summand of $Z(G)$ of maximal order. By Propositions 3.3 and 3.4 applied to H and HA it follows that $|A| = 4$ and H is D_8 or Q_8 or T. Now suppose that $Z(G)$ has a subgroup $A \times B \cong Z_4 \times Z_4$. If $H \cap (A \times B) = 1$ then $H(A \times B) = (H \times A) \times B$ cannot have the small squaring property on 3-sets by Proposition 3.4(b), which is a contradiction. Thus we may assume that $H \cap A \neq \{1\}$. Suppose first that H is D_8 or Q_8. Then $Z(HA) = A$, so that $HA \cap B = 1$. Hence $H(A \times B) = (HA) \times B$ and this does not have the small squaring property on 3-sets by Proposisiton 3.4, a contradiction. Now suppose that $H = T = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^{-1} \rangle$. Then $H(A \times B)$ does not have the small squaring property on 3-sets by Proposition 3.4(c). Thus $Z(G) \cong E \times A$ with E elementary abelian or trivial. ∎

Next we investigate the structure of the derived quotient G/G' of a nonabelian 2-group G with the small squaring property on 3-sets. Let

$$G/G' = \langle aG' \rangle \times \langle c_1G' \rangle \times \ldots \times \langle c_nG' \rangle$$

where $O(aG') \geqslant O(c_1G') \geqslant \ldots . \geqslant O(c_nG')$, (where $O(g)$ denotes the order of g). To obtain restrictions on the orders of the cyclic direct summands we shall examine certain sections of G, for example certain quotients of $\langle a, c_i \rangle$ for some i. We shall need the following lemma which allows us to make use of Proposition 3.3 again.

Lemma 3.6. *Let L be a nonabelian 2-group with derived group L' of order 2. Then $L/Z(L)$ has exponent 2. In particular if L has a generating set of size 2 then L is a minimal nonabelian group.*

Proof: Since $|L'| = 2$ it follows that $L' \subseteq Z(L)$. Let $x, y \in L$. Then $1 = [x, y]^2 = x^{-1}[x, y]y^{-1}xy = [x^2, y]$. Hence $x^2 \in Z(L)$ for all $x \in L$, that is $L/Z(L)$ has exponent 2. Now let $L = \langle a, b \rangle$. Then $L/Z(L) = \langle aZ(L), bZ(L) \rangle$ is elementary abelian of order 4. If H is any subgroup of L of index 2 then H contains $Z(L)$. (For if not then

$L = H\,Z(L)$, so H contains az and bz' for some z, z' in $Z(L)$ and hence H contains $\langle [az, bz'] = [a, b] \rangle = L'$. Then H/L' is a subgroup of $L/L' = \langle aL' \rangle \times \langle bL' \rangle$ of index 2 and so H/L' contains $Z(L)/L' = \langle a^2 L' \rangle \times \langle b^2 L' \rangle$ which contradicts $L = HZ(L)$.) Then since $|H : Z(L)| = 2$ it follows that H is abelian, and hence that L is a minimal nonabelian group. $\square$

Theorem 3.7. *Let G be a nonabelian 2-group with the small squaring property on 3-sets. Then G/G' is either E or $Z_4 \times E$ where E is elementary abelian (or trivial).*

Proof: We use the notation introduced before Lemma 3.6. Note that, since $G' \subseteq \Phi(G)$, we have $G = \langle a, c_1, \dots, c_n \rangle$. Suppose first that $O(aG') \geqslant 8$. Then, by Theorem 3.5, $a \notin Z(G)$, and so for some $i = 1, \dots, n$, $H = \langle a, c_i \rangle$ is nonabelian. Let R be a subgroup of H' of index 2 which is normal in H. By Lemma 3.6, $L = H/R$ is a minimal nonabelian group. Since L has exponent at least 8 it follows from Proposition 3.3 that L does not have the small squaring property on 3-sets, which is a contradiction. Thus $O(aG') = 4$.

Next suppose that $a \in Z(G)$. Then by Theorem 3.5, a has order 4, and it follows that $G \cong \langle a \rangle \times \langle c_1, \dots, c_n \rangle$. By Proposition 3.4(b), $G \cong \langle a \rangle \times Q_8 \times E$ where E is elementary abelian, and so G/G' is the direct product of Z_4 and an elementary abelian group. Thus we may suppose that $a \notin Z(G)$. Suppose that $c_1 G'$ has order 4. Consider $\langle c_1, \dots, c_n \rangle$. If a centralised every element c of this group for which $O(cG') = 4$ then, since the elements of order 4 in the abelian group G/G' generate G/G', it follows that a would centralise $\langle c_1, \dots, c_n \rangle$ and hence a would lie in $Z(G)$. Thus we may assume that $ac_1 \neq c_1 a$. Let $H = \langle a, c_1 \rangle$ and let R be a subgroup of H', of index 2 in H', which is normal in H. Then, by Lemma 3.6, H/R is minimal nonabelian, and by Proposition 3.3, H/R does not have the small squaring property on 3-sets, which is a contradiction. Thus G/G' has the required form. $\square$

Our next task is to examine examples of large exponent. First we deal with those containing an abelian subgroup of index 2.

Proposition 3.8. *Let G be a nonabelian 2-group with the small squaring property on 3-sets. If G has an abelian subgroup A of index 2 with exponent $\exp(A)$ at least 8 then G is a D-group or a Q-group.*

Proof: Let $C = \langle c \rangle$ be a cyclic subgroup of A of order $\exp(A) = 2^n$ say, and let $b \in G - A$. Then $G = \langle b, A \rangle = A \cup bA$. Also, by Theorem 3.5, $c \notin Z(G)$ and hence $bc \neq cb$. Assume first that b^2, c^2 and $(bc)^2$ are all distinct, and consider $K = \{b, c, bc\}$. Now $K^2 \cap bA = \{bc, cb, cbc, bc^2\}$ and these elements are all distinct (for the only possible equality is $cb = bc^2$ which implies $b^{-1}cb = c^2$ whence c and c^2 have the same order, a contradiction). The set $K^2 \cap A = \{b^2, b^2 c, (bc)^2, c^2, bcb\}$ and the only possible equalities between these elements are $b^2 c = c^2$ and $c^2 = bcb$. If

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

$b^2c = c^2$ then $c = b^2$ whence $C_G(c)$ contains $\langle b, A\rangle = G$, that is $c \in Z(G)$ which is a contradiction. If $c^2 = bcb$ then $c^3 = (bc)^2$ whence $C_G(c^3)$ contains $\langle A, bc\rangle = G$, that is c^3 and hence c lie in $Z(G)$, again a contradiction. Thus $|K^2| = 9$ which is not the case. So for any element c of maximal order in A, and any $b \in G - A$, the elements b^2, c^2 and $(bc)^2$ are not all distinct.

Suppose that $b^2 = c^2$ for some such b, c. Then b has order 2^n. Let $L = \langle b, c\rangle$. Then L is nonabelian (recall $bc \neq cb$) and c^2 lies in its centre. So by Theorem 3.5, c^2 has order at most 4. Thus $\exp(A) = 2^n = 8$. We claim that b inverts c. For $d = b^3 \in G - A$ and $d^2 = b^6 = c^6 \neq c^2$ so either $d^2 = (dc)^2$ or $c^2 = (dc)^2$. In the latter case, $c = dcd = d(dcd)d = d^2cd^2 = c^{6+2+6} = c^6$ which is a contradiction. Thus $d^2 = (dc)^2$, that is $d^{-1}cd = c^{-1}$ and it follows that $b = d^3$ inverts c. Similarly, if $(bc)^2 = c^2$ then $\exp(A) = 8$, and bc, and hence b inverts c. Finally if c^2 is not equal to b^2 or $(bc)^2$ then we must have $b^2 = (bc)^2$, and again $b^{-1}cb = c^{-1}$.

Thus we have shown that, for each $b \in G-A$ and each $c \in A$ of order 2^n, b inverts c, and if either $b^2 = c^2$ or $(bc)^2$ for some such b, c, then A has exponent 8. Now, as A is generated by its elements of order 2^n, each element $b \in G - A$ inverts each element of A. In particular, for c of order 2^n in A, $b^2c^{-1} \in A$ and so b inverts c and b^2c^{-1}. Thus we have $b^2c^{-1} = b^{-1}b^2(bc^{-1}) = b^{-1}b^2cb = (b^2c)^{-1} = c^{-1}b^{-2} = b^{-2}c^{-1}$ (as A is abelian), and hence $b^4 = 1$. Thus each element b of $G - A$ has order at most 4. Suppose that some $b \in G - A$ has order 2. Then, for each $a \in A$ we have $(ba)^2 = (bab)a = a^{-1}a = 1$, that is each element of $G - A$ has order 2. In this case G is a D-group. Thus we may assume that each element of $G - A$ has order 4. If $b, d \in G - A$ then $d = ba$ for some $a \in A$ and so $d^2 = b(ab)a = bba^{-1}a = b^2$. Thus G is a Q-group. ∎

Now we complete the classification for the case of large exponent.

THEOREM 3.9. *Let G be a nonabelian 2-group of exponent at least 8 with the small squaring property on 3-sets. Then G is a D-group or a Q-group.*

PROOF: We prove this Proposition by induction on $|G|$. Now $|G| \geqslant 16$ and if $|G| = 16$ then the result follows from Proposition 3.8. So assume that the result is true for groups of order less than $|G|$. Let G have exponent $2^n \geqslant 8$ and let $C = \langle c\rangle$ be a cyclic subgroup of order 2^n in G. By Proposition 3.8 we may assume that G does not contain an abelian subgroup of index 2 and exponent 2^n. Let M be a subgroup of G containing C with $|G : M| = 2$. Then M is not abelian, and by induction M is a D-group or a Q-group. It follows from Lemma 3.2 that M has a characteristic subgroup A of index 2 which is abelian. Thus A is normal in G of index 4.

Suppose that G/A is cyclic, say $G/A = \langle aA\rangle$. By Definition 3.1 and Lemma 3.2, a^2 inverts A and a^2 has order at most 4. Let $K = \{a, c, ac\}$. Then $K^2 \cap A = \{c^2\}$.

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

In the set $K^2 \cap aA = \{ac, ca, ac^2, cac\}$ the only possible equality is $ca = ac^2$ which implies $a^{-1}ca = c^2$. This is impossible since c and c^2 have different orders. Thus $|K^2 \cap aA| = 4$. Also $K^2 \cap a^2A = \{a^2, (ac)^2, a^2c, aca\}$ and the only possible equality between these elements is $a^2 = (ac)^2$, that is $a^{-1}ca = c^{-1}$. However this would imply that a^2 centralised c which is not the case. Hence $|K^2| = 9$ which is a contradiction. Thus G/A is elementary abelian of order 4. Let M_i, $i = 1, 2, 3$, be the subgroups of index 2 in G containing A. As above each M_i is a D-group or a Q-group. Let $M_i = \langle a_i, A\rangle$ for $i = 1, 2, 3$. Suppose that A is not cyclic. Then $A - C$ contains an involution x say, and as a_i inverts A, $a_ix = xa_i$ for each $i = 1, 2, 3$. Hence $x \in Z(G)$. Now $G/\langle x\rangle$ has exponent 2^n (as $C \simeq C\langle x\rangle/\langle x\rangle$), is nonabelian, and is not a D-group or a Q-group (since $A/\langle x\rangle$ is a maximal abelian subgroup of $G/\langle x\rangle$ and it has index 4 and order at least 2^n). This contradicts the inductive assumptions. Thus $A = \langle c\rangle$ is cyclic. If M_i is a D-group then by definition $a_i^2 = 1$ and M_i is dihedral of order 2^{n+1}. If M_i is a Q-group then a_i has order 4 and M_i is a generalised quaternion group of order 2^{n+1}. Thus each of the M_i is a nonabelian 2-group of maximal class (see [**12**, 5.4.5]), and G itself is not of maximal class. Hence the subgroup A is contained in exactly 3 subgroups of G of maximal class and order 2^{n+1}, whereas it was shown in [**2**] that a proper subgroup A of a 2-group G, where G is not of maximal class, is such that A is contained in an even number of subgroups of maximal class and given order $2^r > |A|$. This contradiction completes the proof of Theorem 3.9. □

Finally we obtain a bound on the derived length. Note that each D-group and Q-group has derived length 2.

THEOREM 3.10. *Let G be a nonabelian 2-group with the small squaring property on 3-sets. Then G has derived length 2.*

PROOF: We prove this result by induction on $|G|$. It is certainly true for $|G| = 8$ so we assume that $|G| > 8$ and that the result is true for groups of order less than $|G|$. We may assume that G has exponent 4. Suppose that $G'' \neq 1$. Then G has a normal subgroup R which is elementary abelian of order 4 (see [**13**, III] or [**1**]). Suppose that R is contained in $Z(G)$, and let M_1, M_2 be distinct subgroups of R of order 2. Then by induction $(G/M_1)'' = 1$ and $(G/M_2)'' = 1$ and hence $G'' \leqslant M_1 \cap M_2 = 1$, which is a contradiction. Hence $R \not\leqslant Z(G)$. Now $R \neq \Phi(G)$, for it was shown in [**15**] that a 2-group G with Frattini subgroup $\Phi(G) = Z_2 \times Z_2$ is such that $\Phi(G) \leqslant Z(G)$. If $\Phi(G) \subset R$ then $|\Phi(G)| = 2$ and $G'' = 1$. Hence $R \not\geqslant \Phi(G)$, and so G/R has exponent 4. Also G/R is nonabelian since $G'' \neq 1$. Let $x \in G - R$ be such that $x^2 \notin R$ and consider $L = \langle x, R\rangle$. Then $|L| = 16$ and if L were nonabelian it would be minimal nonabelian (note that x^2 centralises R) and by Proposition 3.3, $L \simeq T = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^{-1}\rangle$ which is not the case. Thus L is abelian, that is x centralises R.

Now consider $A = \langle x \mid O(xR) = 4\rangle$. Then A contains R and $|G : A| \leqslant 2$ (for G/R is nonabelian, and if $A/R \neq G/R$ then the arguments in the proof of Lemma 3.2(a) show that $|G : A| = 2$). Also R centralises each element of A. If $G = A$ then $R \leqslant Z(G)$ which is not the case. Thus $|G : A| = 2$, and so G/R is a D-group. Also $C_G(R) = A$, and $G = \langle A, d\rangle$ for some d such that $d^2 \in R$. Now $d \notin C_G(R)$ and so $\langle d, R\rangle \simeq D_8$ (a nonabelian group of order 8 containing $Z_2 \times Z_2$). Thus $\langle d, R\rangle - R$ contains an involution, and we may assume therefore that $d^2 = 1$. Let $a \in A$ be such that $a^2 \notin R$ (that is $O(aR) = 4$). Let $b \in R - Z(\langle d, R\rangle)$, and let $c = dbd$. Then $Z(\langle d, R\rangle) = \langle bc\rangle$. Since G/R is a D-group it follows from Lemma 3.2 that $dadR = a^{-1}R$. If $dad = a^{-1}b$ then $a = d(dad)d = da^{-1}bd = (dad)^{-1}dbd = (a^{-1}b)^{-1}c = bac = abc$ (since $a \in C_G(R)$), and hence $bc = 1$ which is a contradiction. Similarly $dad \neq a^{-1}c$. Hence dad is either a^{-1} or $a^{-1}bc$.

Suppose that $dad = a^{-1}$, and consider $K = \{a, d, abd\}$. Then $K^2 - A = \{ad, da, a^2bd, abda\}$. If $ad = abda$ then $d = bda = dca$, so $ca = 1$, contradiction. If $da = a^2bd$ then $a^{-1}d = a^2bd$ so that $a^3 = b^{-1} \in R$, contradiction. If $a^2bd = abda = aba^{-1}d$, again a contradiction as a centralises R. Thus $|K^2 - A| = 4$. Also $K^2 \cap A = \{a^2, dabd = a^{-1}c, d^2 = 1, abd^2 = ab, (abd)^2 = bc\}$ has size 5 and so $|K^2| = 9$ which is a contradiction.

Thus $dad = a^{-1}bc$. Consider $K = \{a, d, bd\}$. Here $K \cap R = R$, $K^2 \cap (A - R) = \{a^2\}$, and $K - A = \{ad, da, abd, bda\}$ has order 4. Thus $|K^2| = 9$. This final contradiction completes the proof of Theorem 3.10. □

The main theorem of this section, Theorem 2, now follows immediately from Theorems 3.5, 3.7, 3.9 and 3.10.

3. Groups in which $|K| < 7$ for all $|K^2| = 3$

In this section we prove Theorem 3. Suppose that G is a finite nonabelian group such that $|K^2| < 7$ for all 3-element subsets K of G. We shall prove that G is isomorphic to S_3. Clearly S_3 has this property.

Suppose first that G is a 2-group. Then, as G is not abelian, $G/Z(G)$ is not cyclic and so G has distinct maximal normal subgroups M, N both containing $Z(G)$. Let $a \in M - N$. Then $a \notin Z(G)$ and so a does not centralise $N = \langle N - M\rangle$, so there is an element $b \in N - M$ such that $ab \neq ba$. If $K = \{a, b, ab\}$ than $|K^2| \geqslant 7$ which is a contradiction. Thus G is not a 2-group. By Theorem 1, $G = TP$ where T is an abelian normal odd order subgroup and P is a nontrivial 2-group. Also P contains an element a which inverts T. Suppose that $|T| > 3$ and let $b, c \in T - \{1\}$ be such that $c \neq b$, $c \neq b^{-1}$. Then for $K = \{a, b, c\}$, we have $|K^2| \geqslant 7$ which is a contradiction. Thus $T = \langle b\rangle$ is cyclic of order 3. Also if $a^2 \neq 1$ then for $K = \{a, b, ab\}$ we have

$|K^2| \geqslant 7$. Thus $a^2 = 1$ and $\langle a, b\rangle \simeq S_3$. If $|P| > 2$ then P contains an element c distinct from a such that c inverts T. As above $c^2 = 1$. Then for $K = \{a, b, bc\}$ we have $|K^2| = 8$ which is a contradiction. Thus $|P| = 2$ and $G \cong S_3$.

5. Groups with small cubing on 2-sets

In this section we consider finite groups G with the small cubing property on 2-sets, that is $|K^3| < 8$ for all 2-element subsets K of G. The main result we prove is the following technical theorem.

Theorem 5.1. *Suppose that G is a finite group such that $|K^3| < 8$ for all 2-element subsets K of G. Then the following hold.*

- (a) *The group G has a normal abelian Hall $\{2, 3\}'$-subgroup H.*
- (b) *A Sylow 3-subgroup P of G centralises H. Further either P is abelian, or $H = 1$, P is a nonabelian group of exponent 3 and P contains its centraliser in G that is $C_G(P) = Z(P)$.*
- (c) *If Q is a Sylow 2-subgroup of G then $\langle a^2 \mid a \in Q\rangle$ centralises H.*

An immediate corollary to this result is the complete classification of odd order groups with the small cubing property on 2-sets stated as Theorem 4 in the introduction.

Unfortunately we do not have sufficient information about the Hall $(2, 3)$-subgroups of G to get a classification of the even order examples. This is an open problem. However we are able to obtain the weaker classification, Theorem 5, of finite groups G such that $|K^3| < 6$ for all 2-element subsets K of G.

First we prove Theorem 5.1 in a sequence of lemmas.

Lemma 5.2. *Let G be a finite group, which is not a 2-group, with the small cubing property on 2-sets. Let p be an odd prime dividing $|G|$ and let P be a Sylow p-subgroup of G. Then either P is abelian, or $p = 3$, P has exponent 3, there is a 2-element subset K of P with $|K^3| = 7$, and the centraliser $C_G(P)$ of P is the centre $Z(P)$ of P.*

Proof: Suppose that P is not abelian and let $b \in P - Z(P)$. Then b lies in a maximal normal subgroup N of P, and, as P is generated by $P - N$, there is an element $a \in P - N$ such that $ab \neq ba$. Let $K = \{a, b\}$. Then each of $K^3 \cap aN = \{ab^2, bab, b^2a\}$ and $K^3 \cap a^2N = \{a^2b, aba, ba^2\}$ has size 3. Since $|K^3| < 8$ it follows that $a^3 = b^3$ whence $p = 3$ (for $ab \neq ba$) and $|K^3| = 7$. Similarly by considering $K = \{a, b^2\}$ we obtain $a^3 = b^6$ whence $a^3 = b^3 = 1$. Thus all elements in $P - Z(P)$ have order 3. If now $c \in Z(P)$ then $bc \notin Z(P)$ so $1 = (bc)^3 = b^3c^3 = c^3$. Hence P has exponent 3.

Finally suppose that c is a nontrivial element in $C_G(P) - P$ and consider $K = \{a, bc\} \subset P \times \langle c\rangle$. The sets $K^3 \cap Pc^2$ and $K^3 \cap \left(Pc \cup Pc^3\right)$ have sizes 3 and 4

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

respectively and it follows that $|K^3| = 8$ which is a contradiction. Hence $C_G(P) = Z(P)$. $\square$

LEMMA 5.3. *Let G be an odd order group with the small cubing property on 2-sets. Then (a) and (b) of Theorem 5.1 are true.*

PROOF: Suppose that Theorem 5.1 is false for some odd order group and let G be such a group with minimal order. By Lemma 5.2 it follows that G is not nilpotent. Also, by minimality and Lemma 5.2, each proper subgroup of G is either abelian or a nonabelian group of exponent 3. Suppose first that a Sylow 3-subgroup P of G is nonabelian. Now G is soluble and $G \neq P$. If G/G' is a 3-group, then by minimality G' has a normal abelian Hall $\{2, 3\}'$-subgroup H and H is a Hall subgroup of G. By Lemma 5.2, P does not centralise H and so there are noncommuting elements $a \in P$ and $b \in H$. If $K = \{a, b\}$ then $|K^3| = 8$ which is a contradiction. Thus $|G/G'|$ is divisible by some prime p greater than 3. Then G has a maximal normal subgroup M of index p. Since M contains P it follows from minimality that $M = P$. Let $c \in G$ have order p, and let $K = \{a, b\} \subseteq P$ with $|K^3| = 7$ as in the proof of Lemma 5.2. If c centralised P then $|\{a, bc\}^3| = 8$ which is a contradiction. Hence c does not centralise P, so let $b \in P$ be such that $cb \neq bc$. Then if $K = \{c, b\}$ we have $|K^3| = 8$ which is a contradiction. Thus P is abelian and each proper subgroup of G is abelian. Then by [11] or [18, 9.1.9], $|G| = p^u q^v$ for distinct primes p and q, G has a normal abelian Sylow q-subgroup Q and a cyclic Sylow p-subgroup $\langle a \rangle$. Since G is nonabelian there is an element $b \in Q$ such that $ab \neq ba$. Then if $K = \{a, b\}$ we have $|K^3| = 8$ which is a contradiction. This completes the proof of the lemma. $\square$

LEMMA 5.4. *Let G be an even order group with the small cubing property on 2-sets. Then Theorem 5.1 is true for G.*

PROOF: Suppose that Theorem 5.1 is false for some even order group and let G be such a group with minimal order. Suppose that G is not simple and let N be a maximal normal subgroup of G. By the minimality of G and by Lemma 5.3, N has a normal Hall $\{2, 3\}'$-subgroup H_1. Since H_1 is a characteristic subgroup of N it follows that H_1 is normal in G. Suppose that H_1 is nontrivial. Then, by minimality, G/H_1 has a normal Hall $\{2, 3\}'$-subgroup H/H_1 where $H \supseteq H_1$. It follows that H is a normal Hall $\{2, 3\}'$-subgroup of G, and $H \neq G$ since $|G|$ is even. Then G/H is a $\{2, 3\}$-group and, in particular, G is soluble. Let T be a Hall $2'$-subgroup of G. Then T contains H and, since $H \supseteq H_1 \neq \{1\}$ it follows from Lemma 5.3 that T is abelian. Thus H is abelian, a Sylow 3-subgroup P of G is abelian, and P centralises H. Let Q be a Sylow 2-subgroup of G. If a^2 centralised H for each $a \in Q$ then Theorem 5.1 would be true for G. Thus there are elements $a \in Q$ and $b \in H$ such that $a^2 b \neq ba^2$. But then $|\{a, b\}^3| = 8$. Hence $H_1 = \{1\}$, that is N is a $\{2, 3\}$-group. Now by minimality

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

and Lemma 5.3 the quotient group G/N satisfies the conclusions of Theorem 5.1. In particular G/N is soluble, and since G/N is simple we have $G/N \simeq Z_p$ for some prime p. By minimality a Sylow 3-subgroup of G is abelian or nonabelian of exponent 3. If $p \leqslant 3$ then Theorem 5.1 is true for G and hence $p \geqslant 5$. Thus $|G| = 2^u 3^v p$ and N is the unique maximal normal subgroup of G. Let M be a minimal normal subgroup of G. Then by minimality it follows that G/M has a normal Hall $\{2, 3\}'$-subgroup L/M of order p. If $L \neq G$, then, again by minimality, L has a normal subgroup L_1 of order p. Further L_1 is a normal $\{2, 3\}'$-subgroup of G and (considering the subgroup $L_1 P$) a Sylow 3-subgroup P is abelian and centralises L_1. Also for each 2-element a, a^2 centralises L_1 (consider $K = \{a, b\}$ for $b \in L_1$). Hence Theorem 5.1 is true for G which is a contradiction. Thus $L = G$, and it follows that $N = M$ is a minimal normal subgroup of G and hence is an elementary abelian 2-group. Now G acts irreducibly on N and so a subgroup $\langle a \rangle$ of order p is self-normalising in G. Thus each element of $G - N$ has order p. Let $b \in a^2 N$. If $K = \{a, b\}$ then $|K^3| = 8$ (for $K^3 \cap a^4 N = \{ba^2, a^2 b, aba\}$, $K^3 \cap a^5 N = \{bab, b^2 a, ab^2\}$, $K^3 \cap \langle a \rangle = \{a^3\}$, and neither a nor a^2 commutes with b).

We conclude that G is a simple group, and as Theorem 5.1 is false for G, G is a nonabelian simple group. By Burnside's Theorem [**12**, 4.3.3], $|G|$ is divisible by at least three distinct primes, p, q, r, say, with $p > q > r$. Then $p > q \geqslant 3$. As G is simple it is generated by its elements of order p, and, as G has trivial centre, no non-identity element of G is centralised by all the elements of order p. In particular, for $a \in G$ of order q, there is an element $b \in G$ of order p such that $ab \neq ba$. Let $K = \{a, b\}$. By our assumption, $|K^3| < 8$. Thus $x_1 x_2 x_3 = y_1 y_2 y_3$, where each x_i and y_i is a or b and the triples (x_1, x_2, x_3) and (y_1, y_2, y_3) are distinct. Since $ab \neq ba$, and since a and b have odd order, we must have $x_1 \neq y_1$. Similarly $x_3 \neq y_3$. We may assume that $x_1 = a$ and $y_1 = b$. Suppose first that $x_3 = a$. Then $y_3 = b$. If $x_2 = a$ and $y_2 = b$, then $\langle b \rangle = \langle b^3 \rangle = \langle a^3 \rangle$, which is not the case. Thus if $x_2 = a$ then also $y_2 = a$ and $a^3 = bab$. In this case $a^4 = (ab)^2$, and so $\langle a \rangle = \langle a^4 \rangle = \langle (ab)^2 \rangle \leqslant \langle ab \rangle$; it follows that $\langle a, b \rangle = \langle ab \rangle$ which contradicts the fact that $ab \neq ba$. Therefore $x_2 = b$. If also $y_2 = b$ then $b^3 = aba$ and we get a contradiction as before. So $y_2 = a$ and $aba = bab$. Then $(ba)^{-1} a (ba) = (ba)^{-1} bab = b$, so that a and b are conjugate. This is impossible since a and b have different orders.

Thus $x_3 = b$ and $y_3 = a$. Suppose that $x_2 = a$. Then $a^2 b = b y_2 a$. Since $ab \neq ba$ and a has odd order, $a^2 b \neq ba^2$, and therefore $y_2 = b$ and $a^2 b = b^2 a$. It follows that $b^{-1} a^2 b = b^{-1} b^2 a = ba$, and $a^{-1} b^2 a = ab$. Thus $b^{-2} a^2 b^2 = b^{-1} bab = ab = a^{-1} b^2 a$, which means that a^2 and b^2 are conjugate. This is impossible as a^2 and b^2 have different orders. Hence $x_2 = b$ and $ab^2 = b y_2 a$. Again, as $ab^2 \neq b^2 a$, we must have $y_2 = a$. Then $ab^2 = ba^2$, and hence $(b^{-1})^2 a^{-1} = (a^{-1})^2 b^{-1}$; this leads to a

https://doi.org/10.1017/S0004972700029932 Published online by Cambridge University Press

contradiction as above. This completes the proof of Lemma 5.4. $\square$

Lemmas 5.3 and 5.4 complete the proof of Theorem 5.1. Now we prove Theorem 5.

PROOF OF THEOREM 5: First we show that abelian groups and groups satisfying (a) and (b) have the property that $|K^3| < 6$ for all 2-element subsets K. This is certainly true for abelian groups. Next let $G = \langle a, H\rangle$ where H is abelian of exponent 4 and of index 2 in G, $a^2 = 1$, and $axa = x^{-1}$ for all x in H. Let K be a 2-element subset of G. If $K \subseteq H$ then $|K^3| \leqslant 4$ so assume that K contains an element c of $G - H$. Now $c = ay$ for some y in H. We have $c^2 = y^a y = 1$ and if $x \in H$ then $x^c = (x^a)^y = x^{-1}$ so we may assume that $c = a \in K$. If $K = \{a, x\}$ with $x \in H$ then $K^3 = \{a = a^3 = xax, x = x^3 = axa = a^2x = xa^2, ax^2, ax^2 = x^2a\}$ has order at most 3. Thus we may assume that $K = \{a, ax\}$ for some $x \in H$. Then $K^3 = \{a = a^3 = (ax)^2a = a(ax)^2, ax = a^2(ax) = (ax)a^2 = (ax)^3, ax^2 = (ax)a(ax), ax^3 = a(ax)a\}$ has order at most 4. Finally let G be a 2-group such that $\Phi(G) = \langle x\rangle$ has order 2. Then x is in the centre of G. Let K be a 2-element subset of G. If $x \in K$ then $|K^3| < 6$ so assume that $K = \{a, b\} \subseteq G - \langle x\rangle$. Then a^2 and b^2 lie in $\Phi(G) = \{1, x\} \subseteq Z(G)$ and each element of K^3 is equal to one of a, ax, b, bx. Thus each of the groups in the conclusion of Theorem 5 has the required cubing property.

Now suppose that G is a nonabelian group with the property that $|K^3| < 6$ for all 2-element subsets K. Then G satisfies the conclusions of Theorem 5.1. By Lemma 5.2 a Sylow 3-subgroup P of G is abelian and so a Hall $2'$-subgroup HP of G is abelian. Since G is not abelian $|G|$ is even. Let Q be a Sylow 2-subgroup of G. If there are elements $a \in Q$ and $b \in H$ such that $ab \neq ba$, then, with $K = \{a, b\}$, each of the sets $K^3 \cap (H \cup a^2H)$ and $K^3 \cap (aH \cup a^3H)$ has size at least 3, contradicting the fact that $|K^3| < 6$. Thus Q centralises H, whence H lies in the centre $Z(G)$ of G. Suppose that G has a normal subgroup M of index 3. Then, by minimality, either M is abelian or M is a nonabelian 2-group. We claim that G has a section isomorphic to A_4. Let $G = \langle M, c\rangle$ with $c \in P$. As G is not abelian, and as c centralises PH, in either case c normalises but does not centralise Q. It follows that some section of $\langle Q, c\rangle$ is isomorphic to A_4. However $\{(1\ 2\ 3), (1\ 2)(3\ 4)\}^3$ has order 7. Thus G has no normal subgroup of index 3, and therefore a maximal normal subgroup M of G, with $H \leqslant M$, has index 2 in G. Suppose now that $PH \neq 1$. Then, by minimality, M is abelian, whence $M = PH \times (M \cap Q)$. Let $G = \langle M, c\rangle$ with $c \in Q$. If $ca \neq ac$ for some $a \in PH$, then, with $K = \{a, c\}$, each of the sets $K^3 \cap (PH \cup a^2PH)$ and $K^3 \cap (aPH \cup a^3PH)$ has size at least 3, contradicting $|K^3| < 6$. Thus c centralises PH and we have $G = PH \times Q$, whence Q is nonabelian and $ca \neq ac$ for some $a \in Q$. Then, if $b \in (PH) \setminus \{1\}$ and $K = \{ab, c\}$, we have $|K^3| \geqslant 6$ (noting that the sets $\{c^3, a^3b^3\}$, $\{(ab)^2c, abcab\}$, and $\{abc^2, cabc\}$ are each of size 2 and are disjoint, as they lie in disjoint unions of cosets of Q). Thus $PH = 1$ and G is a nonabelian 2-group.

If $|K^2| < 4$ for all 2-element subsets of G then Theorem 5(b) is true by [9] so we may assume that for some $K = \{a, b\}$ we have $|K^2| = 4$. For such 2-element subsets K we consider Table 1 below,

	a^2	ab	ba	b^2
a	a^3	a^2b	aba	ab^2
b	ba^2	bab	b^2a	b^3

Table 1

called a third stage multiplication table in [4]. We write $A = a^3$, $B = a^2b$, $C = aba$, $D = ab^2$. Then according to the analysis in [4], since $|K^2| = 4$ and $|K^3| < 6$, the second row (ba^2, bab, b^2a, b^3) of Table 1 is one of (B, A, D, C), (D, A, E, C), (D, C, B, A) and (E, A, B, C) where $E \in G$ is distinct from A, B, C, D. Let us temporarily call these types 1, 2, 3 and 4 respectively. We will show that only type 1 is possible.

Suppose first that K is of type 2, that is $a^3 = bab$, $aba = b^3$, and $ab^2 = ba^2$. It follows that, for $L = \{a^2, b\}$, $|L^2| = 4$. If L is of type 1, 2 or 4, then $a^6 = ba^2b$ which in turn is equal to ab^3, whence $a^5 = b^3 = aba$ so that $b = a^3$ and hence $ab = ba$, which is a contradiction. Thus L is of type 3, so $a^6 = b^3$ which equals aba, whence $a^4 = b$ and $ab = ba$, again a contradiction.

Next suppose that K is of type 3, that is $ab^2 = ba^2$, $aba = bab$, $a^2b = b^2a$, and $a^3 = b^3$. Again it follows that $|L^2| = 4$ for $L = \{a^2, b\}$. If L is of type 1, 2 or 4 then $a^6 = ba^2b$ which equals ab^3, whence $a^5 = b^3 = a^3$ and so $a^2 = 1$ which contradicts the fact that $|L^2| = 4$. Thus L is of type 3 so $a^2b^2 = ba^4$ which equals $ab^2a^2 = abab^2$ whence $b = 1$ which is a contradiction.

Finally suppose that K is of type 4, that is $a^3 = bab$, $a^2b = b^2a$, and $aba = b^3$. Again we find that $|L^2| = 4$ for $L = \{a^2, b\}$ and arguing as above leads to a contradiction.

Thus any $K = \{a, b\}$ such that $|K^2| = 4$ is of type 1, that is $a^3 = bab$, $a^2b = ba^2$, $ab^2 = b^2a$, $aba = b^3$. Since for such a set $K = \{a, b\}$ we have $ab \neq ba$, certainly $a^2b \neq aba$. If $a^2 \neq (ab)^2$ then $L = \{a, ab\}$ is also of type 1 and so $a^3 = (ab)a(ab) = a^3b^2$, that is $b^2 = 1$. On the other hand if $a^2 = (ab)^2$ then $a^2 = a(bab) = a^4$, that is $a^2 = 1$. Thus, for each $K = \{a, b\}$ such that $|K^2| = 4$, either $a^2 = 1$ or $b^2 = 1$.

We claim that G has exponent 4. Let $K = \{a, b\}$ have $|K^2| = 4$ and suppose that $b^2 = 1$. Then $a^6 = (bab)^2 = ba^2b = a^2$ so that $a^4 = 1$, and as $a^2 \neq b^2 = 1$, a has order 4.

Now suppose that there is an $x \in G$ with $x^4 \neq 1$. Then $|\{a, x\}^2| < 4$ and as x^2 (of order at least 4) is not equal to a^2 we must have $ax = xa$. Similarly $bx = xb$. But then $|\{a, bx\}^2| = 4$ while $a^2 \neq 1$ and $(bx)^2 = x^2 \neq 1$, which is a contradiction. Thus G has exponent 4.

Suppose that, for each pair a, b of non-commuting elements of G either $a^2 = 1$ or $b^2 = 1$. Then $A = \langle x \mid x^2 \neq 1 \rangle$ is an abelian subgroup of G. Let $a \in G - A$. Then $a^2 = 1$, and if $x \in A$ then $ax \in G - A$ and so $(ax)^2 = 1$, that is $x^a = x^{-1}$. Thus each element of $G - A$ inverts A. Further G/A is elementary abelian. If $|G/A| \geqslant 4$ then there are elements a, b, ab in $G - A$ lying in distinct cosets of A and it is not possible for each of a, b and ab to invert A. Thus $|G : A| = 2$. Finally, as G has exponent 4, A has exponent 4 and so G satisfies (b)(i) of the theorem.

Thus we may suppose that there is a pair a, b of non-commuting elements such that $a^2 = b^2 \neq 1$. We claim that $\Phi(G) = \langle x^2 \mid x \in G \rangle$ has order 2. Suppose that there is an $x \in G$ such that $1 \neq x^2 \neq a^2$. Then $\left|\{a, x\}^2\right| < 4$ and so $ax = xa$. Similarly $bx = xb$. Also $(bx)^2 = b^2x^2 = a^2x^2 \neq a^2$ and $(bx)a = ba\,x \neq abx$ and so $\left|\{a, bx\}^2\right| = 4$ while $a^2 \neq 1$ and $(bx)^2 = a^2x^2 \neq 1$. This is a contradiction and so $\Phi(G) = \langle a^2 \rangle$ has order 2 and (b)(ii) of the theorem is true. This completes the proof of Theorem 5. $\square$

REMARK. Nekrasov [16] proved that a finite nonabelian group with the property that, for each $K = \{a, b\}$ with $\left|K^2\right| = 4$, the equalities $a^3 = bab$, $a^2b = ba^2$, $ab^2 = b^2a$ and $aba = b^3$ hold, satisfies part (b) of Theorem 5; the last part of our proof of Theorem 5 is basically due to him.

REFERENCES

[1] Ya. G. Berkovich, 'On p-groups of finite order', *Siberian Math. J.* **9** (1968), 1284–1306. (in Russian; English translation) .

[2] Ya. G. Berkovich, 'Generalization of theorems of P. Hall and Blackburn and an application to non-regular p-groups', *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 800–831. (in Russian; English translation) .

[3] Ya. G. Berkovich and G.A. Freiman, 'Group structure and cardinality of powers of its small subsets', (unpublished manuscript, 1981).

[4] L.V. Brailovsky and G.A. Freiman, 'On two-element subsets in groups', *Ann. New York Acad. Sci.* **373** (1981), 183–190.

[5] L.V. Brailovsky and G.A. Freiman, 'On a product of finite subsets in a torsion-free group', *J. Algebra* **130** (1990), 462–476.

[6] L.V. Brailovsky and G.A. Freiman, 'Groups with small cardinality of their two-element subsets', *Ann. New York Acad. Sci* **410** (1983), 75–82.

[7] G.A. Freiman, *Foundations of a structural theory of set addition*, (in Russian) (Kazan, 1966). *Translations of Mathematical Monographs* 37, (English translation) (Amer. Math. Soc., Providence, R.I., 1973).

[8] G.A. Freiman, 'Groups and the inverse problems of the additive set theory', in *Number-theoretic investigations on the Markov spectrum and the structure theory of set addition*, (in Russian), pp. 175–183 (Kalinin University, Moscow, 1973).

[9] G.A. Freiman, 'On two- and three-element subsets of groups', *Aequationes Math.* **22**

(1981), 140–152.

[10] G.A. Freiman and B.M. Schein, 'Group and semigroup theoretic considerations inspired by inverse problems of the additive number theory', in *Lecture Notes in Math.* 1320, pp. 121–140 (Springer-Verlag, Berlin-Heidelberg-New York, 1988).

[11] J.A. Golfand, 'On groups all of whose subgroups are special', *Dokl. Akad. Nauk SSSR)* **60, No. 8** (1948), 1313–1315.

[12] D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).

[13] B. Huppert, *Endliche gruppen I* (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[14] J.H.B. Kemperman, 'On complexes in a semigroup', *Indag. Math.* **18** (1956), 247–254.

[15] K.G. Nekrasov and Ya.G. Berkovich, 'A necessary and sufficient condition for the cyclicity of the Frattini subgroup of a finite p-group, Voprosyteorii Grup, Gomologicheskoi algebry, Yaroslarl', pp. 55–57, (1985).

[16] K.G. Nekrasov, private communication, 1987.

[17] P.M. Neumann, private communication, 1989.

[18] D.J.S. Robinson, *A course in the theory of groups* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

Department of Mathematics
Bar-Ilan University
52900 Ramat-Gan
Israel

School of Mathematical Sciences
Raymond and Beverley Sackler
Faculty of Exact Sciences
Tel-Aviv University
Ramat - Aviv 69978
Israel

Department of Mathematics
University of Western Australia
Nedlands WA 6009
Australia