ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 329–340

ON A COMBINATORIAL PROBLEM IN GROUP THEORY

BY

MARCEL HERZOG*

School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel-Aviv University, Tel-Aviv, Israel

AND

PATRIZIA LONGOBARDI AND MERCEDE MAJ

Dipartimento di Matematica e Appl.ni, Universita' degli Studi di Napoli
Monte S. Angelo, via Cinthia, 80126 Napoli, Italy

Dedicated to John G. Thompson, the Wolf Prize Laureate in Mathematics for 1992

ABSTRACT

We say that a group $G \in DS$ if for some integer m, all subsets X of G of size m satisfy $|X^2| < |X|^2$, where $X^2 = \{xy| \ x, y \in X\}$. It is shown, using a previous result of Peter Neumann, that $G \in DS$ if and only if either the subgroup of G generated by the squares of elements of G is finite, or G contains a normal abelian subgroup of finite index, on which each element of G acts by conjugation either as the identity automorphism or as the inverting automorphism.

1. Introduction

This paper concerns groups in which the subsets of a given size have deficient squares. To make this more precise, let G be a group and let m be an integer, $m > 1$. We say that G belongs to the class $DS(m)$ if for each subset X of G of cardinality m, the subset $X^2 = \{xy| \ x, y \in X\}$ has cardinality less than m^2. In particular, every group of order less then m^2 belongs to $DS(m)$.

* The first author wishes to thank the Department of Mathematics in the University of Napoli for their hospitality during the preparation of this paper.
Received July 1, 1992

Denote by DS the class of groups $\bigcup_{m>1} DS(m)$. In 1989, Peter Neumann [10] proved the following theorem:

THEOREM 1: *If the group G belongs to DS then G is finite-by-abelian-by-finite.*

The aim of this paper is to completely classify the DS-groups. Our proof relies on Theorem 1 and by Peter Neumann's permission we shall include his beautiful proof in our paper.

In order to state our results we need the notion of a nearly-dihedral group. A group G will be called **nearly-dihedral** if it contains a normal abelian subgroup H of finite index, on which each element of G acts by conjugation either as the identity automorphism or as the inverting automorphism. Moreover, denote by $G^{(k)}$ the subgroup of G generated by the k-powers of all elements of G. Our main result is

THEOREM 2: *The group G belongs to DS if and only if either G is nearly-dihedral or $G^{(2)}$ is of finite order.*

The "if" direction of Theorem 2 is easy to prove, and our main effort will be concentrated on proving the "only if" direction. We shall deal separately with groups which satisfy the FC-condition and those which do not satisfy it. Thus we shall prove

THEOREM A: *Let G be an FC-group. Then G belongs to DS if and only if either G is central-by-finite or $G^{(2)}$ is of finite order.*

and

THEOREM B: *Let G be a non-FC-group. Then G belongs to DS if and only if G is nearly-dihedral.*

In particular it follows that a group which belongs to DS is either abelian-by-finite or finite-by-elementary-abelian.

Groups which belong to $DS(m)$ were first considered by G.A.Freiman in [5], motivated by his number-theoretical results on set addition. Freiman proved that a group G belongs to $DS(2)$ if and only if G is either abelian or a non-abelian 2-group with all subgroups normal in G. Recently, groups belonging to $DS(3)$ were completely classified in two complementary papers: J.A.Berkovich, G.A.Freiman and Cheryl E.Praeger [2] and P.Longobardi and M.Maj [6].

This paper will be organized as follows. Section 2 will be devoted to Peter Neumann's proof of Theorem 1. In Section 3 the "if" part of Theorems 2, A and B will be proved, as well as some other preliminary results. The proof of Theorem A will be completed in Section 4 and Theorem B will be proved in Section 5. Finally, Section 6 will be devoted to a discussion of bounds for the finite quantities which appear in the statement of our results.

Our notation is standard. In particular, if S is a subset of a group G, then $\langle S\rangle$ denotes the subgroup of G generated by S, G' denotes the commutator subgroup of G and the center of G is denoted by $Z(G)$. A group G is called **finite-by-abelian-by-finite** if it contains a normal subgroup N of finite index with N' of finite order. A group is called an **FC-group** if all its conjugacy classes are of finite size. In particular, G is an FC-group if G' is of finite order. The **FC-center** of a group G consists of all elements of G with a finite number of conjugates. The FC-center of G is a characteristic subgroup of G.

We wish to thank Peter Neumann for the permission to include Theorem 1 in this paper and for his useful suggestions, including the final formulation of Theorem 2. We wish also to thank Cheryl Praeger for bringing the theorem of Peter Neumann to our attention.

2. Proof of Theorem 1

As indicated in the Introduction, this proof is due to Peter Neumann. For an element g of the group G we define:

$$k_G(g) =_{def} k(g) =_{def} |G : C_G(g)| = \text{number of conjugates of } g.$$

The heart of the matter of the proof is contained in the following lemma.

LEMMA 2.1: *Let G be a group, k and t positive integers, and let $S =_{def} \{g \in G \mid k(g) \leq k\}$. Suppose that there exist $x_1, \ldots, x_t$ in G such that $G = Sx_1 \cup \cdots \cup Sx_t$. If $H =_{def} \langle S\rangle$ then $|H'|$ is bounded by a function of k and t.*

Proof: If $x_i \in H$ then $Sx_i \subseteq H$, whereas if $x_i \notin H$ then, since $Sx_i \subseteq Hx_i$ and $Hx_i \cap H = \emptyset$, we have $Sx_i \cap H = \emptyset$; thus $H = \bigcup\{Sx_i | x_i \in H\}$. We may suppose that $x_1, \ldots, x_s \in H$ and $x_{s+1}, \ldots, x_t \notin H$, so that $H = Sx_1 \cup \cdots \cup Sx_s$. Define $k_i = k(x_i)$. We may certainly rearrange $x_1, \ldots, x_s$ to get $k_1 \leq k_2 \leq \cdots \leq k_s$. Since $1 \in Sx_j$, that is $x_j^{-1} \in S$ (whence $x_j \in S$), for some j, we have $k_j \leq k$ and therefore $k_1 \leq k$. Furthermore, if $x \in Sx_i$ then $x = yx_i$ for some $y \in S$ and so $k_i/k \leq k(x) \leq kk_i$, since $k(wz) \leq k(w)k(z)$ for any $w, z \in G$.

We claim that if $i < s$ then $k_{i+1} \leq k^3 k_i$. For, suppose there exists $j < s$ such that $k_{j+1} > k^3 k_j$. Let $H_0 =_{def} \cup_{i \leq j} Sx_i$; if $x \in H_0 S$, say $x = yz$ with $y \in H_0$ and $z \in S$, then $k(x) \leq k(y)k(z) \leq kk_j k$, so $k(x) \leq k^2 k_j$. On the other hand, if $x \in H - H_0$ then $k(x) \geq k_{j+1}/k > k^2 k_j$ and thus $H_0 S \subseteq H_0$. But this implies that $H_0 = \langle S \rangle = H$, which is false.

Since $k_{i+1} \leq k^3 k_i$ for all $i < s$ we have that $k_i \leq k^{3i-3} k_1 \leq k^{3i-2}$ and so $k_s \leq k^{3s-2}$. Consequently $k(x) \leq k^{3s-1}$ for all $x \in H$. In particular, $k_H(x) \leq k^{3s-1}$ and so H is a BFC-group (i.e. H has boundedly finite conjugacy classes) with the BFC-number $\gamma \leq k^{3s-1}$. It is a famous old theorem of B.H.Neumann (see [7] or [13], p.427) that BFC-groups have finite commutator subgroups. The best known quantitative version of this result is somewhat technical and is due to Cartwright [4]; a slightly less good, but also less technical theorem is to be found in [11], namely that $|H'| \leq \gamma^{\frac{1}{2}(3+5\log_2 \gamma)}$. Thus in our group we find that

$$|H'| \leq k^{\frac{5}{2}(3s-1)^2 \log_2 k + \frac{3}{2}(3s-1)} .$$

Proof of Theorem 1: Suppose that G belongs to $DS(m)$, $m > 1$ and let

$$S =_{def} \{g \in G |\ k(g) \leq m^2(m-1)^2\} .$$

We propose to show that G may be covered by $m - 1$ translates of S. We do this by supposing not and seeking a contradiction. Choose $y_1 \in G$ arbitrary and if $y_1, \ldots, y_j$ have already been chosen, with $j < m$, choose $y_{j+1} \in G - \bigcup_{i=1}^{j} Sy_j$. This is possible precisely because of our supposition that G is not a union of $m-1$ (or fewer) translates Sy_i of S. Thus we obtain $y_1, \ldots, y_m$ with the property that if $i < j$ then $y_j y_i^{-1} \notin S$. Then also, since $y_j^{-1} y_i$ is conjugate to $y_i y_j^{-1}$ and since S is closed under inverses, we find that $y_j y_i^{-1}$ and $y_j^{-1} y_i$ have more than $m^2(m-1)^2$ conjugates whenever $i \neq j$. Let $\Gamma =_{def} \{y_j y_i^{-1} | i \neq j\}$ and $\Delta =_{def} \{y_j^{-1} y_i | i \neq j\}$. Applying Theorem 2 of [3] to G acting on itself by conjugation we find that there exists $x \in G$ such that $x^{-1} \Delta x \cap \Gamma = \emptyset$. This means that if $i_1 \neq j_1$ and $i_2 \neq j_2$ then $x^{-1} y_{j_1}^{-1} y_{i_1} x \neq y_{j_2} y_{i_2}^{-1}$. This inequality also holds of course if $i_1 = j_1$ but $i_2 \neq j_2$, or if $i_1 \neq j_1$ and $i_2 = j_2$; therefore it holds as long as $(i_1, i_2) \neq (j_1, j_2)$. Sorting it out we find that

$$y_{i_1} x y_{i_2} \neq y_{j_1} x y_{j_2}$$

and so $xy_{i_1}xy_{i_2} \neq xy_{j_1}xy_{j_2}$ unless $i_1 = j_1$ and $i_2 = j_2$. Thus if $X =_{def} \{xy_1, \ldots, xy_m\}$ then $|X^2| = m^2$. But this contradicts our hypothesis that G satisfies $DS(m)$ and so we have that there exist $x_1, \ldots, x_{m-1}$ such that $G = Sx_1 \cup \cdots \cup Sx_{m-1}$.

Let $H =_{def} \langle S \rangle$; then clearly $H \trianglelefteq G$, $|G : H| \leq m - 1$ and by Lemma 2.1 $|H'|$ is finite. The proof is complete. ∎

COROLLARY 2.2: *If the FC-group G belongs to DS, then G is finite-by-abelian.*

Proof: Using the above notation, it follows from $G = Sx_1 \cup \cdots \cup Sx_{m-1}$ that G is a BFC-group and hence $|G'|$ is finite. ∎

3. Preliminary Results

The "if" parts of Theorems 2, A and B follow immediately from the following lemma:

LEMMA 3.1: *Let G be a group and let n be a positive integer. If either $|G^{(2)}| = n$ or G contains a normal abelian subgroup H of index n on which each element of G acts by conjugation either as the identity automorphism or as the the inverting automorphism, then G belongs to $DS(n+1)$.*

Proof: Let $X \subseteq G$ with $|X| = n + 1$. If $|G^{(2)}| = n$, then there exist $x, y \in X$, $x \neq y$, such that $x^2 = y^2$ and hence $|X^2| < (n+1)^2$. If G satisfies the second condition, then there exist $x, y \in X$, $x \neq y$, such that $xH = yH$ and so $x = yh$ with $h \in H$. If y centralizes H then $xy = yhy = yyh = yx$ and if y inverts H then $x^2 = yhyh = yyh^{-1}h = y^2$. In any case $|X^2| < (n+1)^2$, thus proving the lemma. ∎

Our next result in this section deals with a sufficient condition for a group not to belong to DS.

LEMMA 3.2: *Let G be a group and suppose that there exists an infinite sequence $\{x_1, \ldots\}$ of elements of G such that*

(I) *$x_i x_j \neq x_j x_i$ for $i \neq j$, and*

(II) *$x_i^2 \neq x_j^2$ for $i \neq j$. Then G does not belong to DS.*

Proof: Following [1], a subset S of G is called a **Sidon set of the first kind** if for $x, y, z, w \in S$ of which at least three are different, $xy \neq zw$. By Proposition 8.1 in [1] every infinite subset of G contains an infinite subset which is a Sidon set of the first kind. Thus we may assume that our sequence has that property, in addition to (I) and (II). For each integer n, $n \geq 2$, define $X_n = \{x_i | i = 1, \ldots, n\}$. Then $|X_n| = n$ and $|X_n^2| = n^2$. Thus G does not belong to DS. ∎

The following lemma is needed for the proof of Theorem A.

LEMMA 3.3: *Let G be an FC-group which belongs to DS. Suppose that H is a subgroup of G and $G = H \times \langle x \rangle$ for some $x \in G$ of infinite order. Then H is central-by-finite.*

Proof: Suppose that H is not central-by-finite. Then by a theorem of B.H.Neumann [9] there exists an infinite sequence $\{y_1, \ldots, y_n, \ldots\}$ of elements of H such that $y_i y_j \neq y_j y_i$ for $i \neq j$.

Define $x_i = y_i x^{3^i}$ for $i = 1, 2, \ldots$. Then, as G belongs to $DS(m)$ for some $m > 1$, it follows from $|\{x_1, \ldots, x_m\}| = m$ that $|\{x_1, \ldots, x_m\}^2| < m^2$ and $x_i x_j = x_h x_k$ for some $1 \leq i, j, k, l \leq m$ with $i \neq h$ and $j \neq k$. Thus $y_i y_j x^{3^i + 3^j} = y_h y_k x^{3^h + 3^k}$ yielding $i = k$ and $j = h$. But then $y_i y_j = y_j y_i$ and $i = j = h$, a contradiction. ∎

We conclude this section with two results which are needed for the proof of Theorem B.

LEMMA 3.4: *Let G be a group which belongs to DS and suppose that $G = A\langle x \rangle$, where A is an abelian normal subgroup of G and $[A, x^2] = 1$. If $a \in A$ has infinite order, then either aa^x or $a^{-1}a^x$ has finite order. In particular, if A is torsion-free, then x acts on A by conjugation either as the identity automorphism or as the inverting automorphism.*

Proof: Let $c =_{def} aa^x$ and assume that c has infinite order. If $\langle c \rangle \cap \langle a \rangle = 1$, consider the elements $a_i =_{def} a^{2^i} x$, $i = 1, \ldots$. Since G belongs to $DS(m)$ for some $m > 1$ and since $|\{a_1, \ldots, a_m\}| = m$, it follows that $a_i a_j = a_h a_k$ for some $1 \leq i, j, h, k \leq m$ with $i \neq h$ and $j \neq k$. Thus $a^{2^i} x a^{2^j} x = a^{2^h} x a^{2^k} x$, whence it follows that $a^{2^i - 2^j} c^{2^j} = a^{2^h - 2^k} c^{2^k}$ and $j = k$, a contradiction. Therefore $\langle c \rangle \cap \langle a \rangle \neq 1$ and $a^n \in \langle c \rangle$ for some $n > 0$. Since $a = a^{x^2}$, it follows that $c^x = c$ and hence $1 = [a^n, x] = [a, x]^n$. Thus $a^{-1}a^x$ has finite order.

If A is torsion free and $a \in A$, then either $a^x = a$ or $a^x = a^{-1}$. Suppose that $a, b \in A - \{1\}$ and $a^x = a$ while $b^x = b^{-1}$. Then $(ab)^x = ab^{-1}$ with $ab^{-1} \notin \{ab, (ab)^{-1}\}$, a contradiction. Thus by conjugation x either fixes A or inverts A, as claimed. ∎

LEMMA 3.5: *Let G be a group which belongs to DS and suppose that $G = A\langle x\rangle$, where A is a periodic normal abelian subgroup of G and $[A, x^2] = 1$. Then there exists a finite subgroup C of A which is normal in G such that either $a^x C = a^{-1}C$ for every $a \in A$ or $a^x C = aC$ for every $a \in A$.*

Proof: Let $s \geq 1$ be maximal such that there exist $a_1, \ldots, a_s \in A$ satisfying

(1) $a_i \notin \langle a_1, \ldots, a_{i-1}\rangle^G$ and

(2) $|\{a_1 x, \ldots, a_s x\}^2| = s^2$.

Such an s exists since G belongs to DS. For every $a = a_{s+1} \in A - \langle a_1, \ldots, a_s\rangle^G$ we have $|\{a_1 x, \ldots, a_s x, a_{s+1}x\}^2| < (s+1)^2$ and hence $a_i x a_j x = a_h x a_k x$ for some $1 \leq i, j, h, k \leq s+1$ with $i \neq h$ and $j \neq k$. Thus $a_i a_j^x = a_h a_k^x$ and by our assumptions we must have $s+1 \in \{i, j, h, k\}$. We may assume that $k = s+1$. By the choice of a_{s+1}, we must have either $i = s+1$ or $h = s+1$, but not both since $i \neq h$. Define $C = \langle a_1, \ldots, a_s\rangle^G$. Since $a_i a_j^x = a_h a_k^x$, we have either $a_{s+1}^x C = a_{s+1}C$ or $a_{s+1}^x C = a_{s+1}^{-1}C$. Thus $A = \{a | a^x C = aC\} \cup \{a | a^x C = a^{-1}C\}$ and since a group cannot be a union of two proper subgroups, A must be equal to one of the subgroups. Finally, C is a finite group since A is a periodic normal abelian subgroup of G and $[A, x^2] = 1$. ∎

4. Proof of Theorem A

By Lemma 3.1 we need only to prove the "only if" part of Theorem A. So suppose that G is an FC-group which belongs to DS and assume, by contradiction, that both $|G/Z(G)|$ and $|G^{(2)}|$ are infinite. It follows from Corollary 2.2 that $|G'|$ is finite. Consequently, $G/Z(G)$ is of finite exponent (see the proof of Theorem 1.4 in [14]).

First assume that $G^{(2)}$ is not finitely generated. Then we shall construct an infinite sequence $\{x_1, x_2, \ldots, x_n, \ldots\}$ of elements of G, such that

(I) $x_i x_j \neq x_j x_i$ for $i \neq j$;

(II) $x_i^2 \neq \langle x_1, \ldots, x_{i-1}\rangle^G$ for every i;

(III) $G \neq C_G(x_1) \cup \cdots \cup C_G(x_i)$ for every i.

Choose an arbitrary $x_1 \in G - Z(G)$ and if $x_1, \ldots, x_i$ have already been chosen, define H,C,A and B by $H = \langle x_1, \ldots, x_i\rangle^G$, $C = G - (C_G(x_1) \cup \cdots \cup C_G(x_i))$, $A = \{g \in C | g^2 \in H\}$ and $B = \{g \in C | g^2 \notin H\}$. Clearly

$$G = C_G(x_1) \cup \cdots \cup C_G(x_i) \cup \langle A\rangle \cup \langle B\rangle.$$

If $|G : \langle A\rangle|$ is finite, say $G = \langle A\rangle \cup y_1\langle A\rangle \cup \cdots \cup y_t\langle A\rangle$, define $K = G'H\langle y_1, \ldots, y_t\rangle$. Then $g^2 \in K$ for every $g \in G$ and $G^{(2)} \leq K$ is finitely generated, a contradiction.

Hence $|G : \langle A\rangle|$ is infinite and by a theorem of B.H.Neumann (see [8]) we get:

$$G = C_G(x_1) \cup \cdots \cup C_G(x_i) \cup \langle B\rangle .$$

Since (III) holds, it follows by the same theorem that $|G : \langle B\rangle|$ is finite.

Suppose that $G = C_G(x_1) \cup \cdots \cup C_G(x_i) \cup C_G(b)$ for every $b \in B$. Since $B \subseteq C$ it follows that $B \subseteq C_G(b)$ for every $b \in B$ and hence $\langle B\rangle$ is abelian and G is abelian-by-finite. But then, by Lemma 2 in [9], $|G : Z(G)|$ is finite, a contradiction.

Thus there exists $b' \in B$ such that $G \neq C_G(x_1) \cup \cdots \cup C_G(x_i) \cup C_G(b')$ and the sequence $x_1, \ldots, x_i, x_{i+1} = b'$ satisfies (I), (II) and (III). It follows by Lemma 3.2 that G does not belong to DS, a contradiction.

Thus $G^{(2)}$ is finitely generated. Since $|G^{(2)}|$ is infinite, G is non-periodic. Denote by T the torsion subgroup of G. As $T \geq G'$, G/T is a torsion-free abelian group with a finitely generated subgroup $G^{(2)}T/T$, whose quotient is an elementary abelian 2-group. Thus G/T is finitely generated. Since $G/Z(G)$ is of finite exponent, say e, we have $x^e \in Z(G)$ for every $x \in G - T$ and applying Lemma 3.3 to $T\langle x^e\rangle = T \times \langle x^e\rangle$ we conclude that T is central-by-finite. Therefore $G/Z(T)$ is a finitely generated FC-group and hence $G/(Z(G)Z(T))$ is finite. But $Z(G)Z(T)$ is abelian and so G is abelian-by-finite. As above, we conclude that G is central-by-finite, a final contradiction.

5. Proof of Theorem B

By Lemma 3.1 we need only to prove the "only if" part of Theorem B. So suppose that G is a non-FC-group which belongs to DS and denote by F its FC-center. The following result shows that the FC-center plays a central role in every group which belongs to DS.

PROPOSITION 5.1: *Let G be a non-FC-group which belongs to DS and let F denote its FC-center. Then $|G : F| = 2$.*

Proof: Since G belongs to DS, there exists a maximal $s \geq 1$ with the following property: there exist $x_1, \ldots, x_s \in G - F$ such that $|\{x_1, \ldots, x_s\}^2| = s^2$. Write

$A = \{x_i x_j \notin F\}$ and $B = \{x_i x_j \in F\}$, where $1 \leq i, j \leq s$. If $x \in G - F$ then by the maximality of s we have $x \in X_1 \cup X_2 \cup X_3 \cup X_4$, where

$$X_1 = \{x | x = x_i x_j x_k^{-1} \text{ or } x = x_i^{-1} x_j x_k\},$$

$$X_2 = \{x \in G | x^{-1} x_i x = x_j\},$$

$$X_3 = \{x \in G | x^2 = x_i x_j \in A\} \text{ and}$$

$$X_4 = \{x \in G | x^2 = x_i x_j \in B\}$$

and $1 \leq i, j, k \leq s$. Thus $G = F \cup X_1 \cup X_2 \cup X_3 \cup X_4$, where X_1 is a finite set, X_2 is the union of a finite number of cosets of $C_G(x_i)$, $1 \leq i \leq s$ and $X_3 \subseteq \cup_{a \in A} C_G(a)$. Hence

$$G = F \cup X_1 \cup X_2 \cup \bigcup_{a \in A} C_G(a) \cup \langle X_4 \rangle .$$

Since $|G : C_G(x_i)|$ and $|G : C_G(a)|$ are infinite for $1 \leq i \leq s$ and $a \in A$, it follows by a theorem of B.H.Neumann [8] that $G = F \cup \langle X_4 \rangle$ and since $G \neq F$, we conclude that $G = \langle X_4 \rangle$.

Let $S =_{def} \langle B \rangle^G$. Then S is a finitely generated subgroup of F. If $x, y \in X_4$ then $x^2, y^2 \in S$ and either $xy \in X_4$, whence $(xy)^2 \in S$, or $x \in Fy^{-1} \cup X_1 y^{-1} \cup X_2 y^{-1} \cup X_3 y^{-1}$. If $(xy)^2 \in S$ then, since $x^2, y^2 \in S$, we conclude that $[xS, yS] = S$ and $x \in C$, where C/S denotes the centralizer of yS in G/S. Since x is an arbitrary element of X_4, we conclude that

$$G = F \cup X_1 \cup X_2 \cup X_3 \cup Fy^{-1} \cup X_1 y^{-1} \cup X_2 y^{-1} \cup X_3 y^{-1} \cup C$$

and again by the theorem of B.H.Neumann we may conclude that $G = F \cup Fy^{-1} \cup C$. It follows that $G = F \langle y \rangle \cup C$ with $y^2 \in F$. If $G = F \langle y \rangle$ then $|G : F| = 2$, as claimed. So assume that $G = C$. Then $Sy \in Z(G/S)$ and since y was an arbitrary element of X_4 and X_4 generates G, we conlude that G/S is an abelian group. Moreover, since $y^2 \in S$ for each $y \in X_4$, G/S is an elementary abelian 2-group.

Since G is not an FC-group, we conclude that S is a finitely generated infinite FC-group which belongs to DS. By Theorem A $|S : Z(S)|$ is finite, forcing $Z(S)$ to be an abelian finitely-generated infinite group. Thus $Z(S) = Y \times K$, where Y is a nontrivial finitely-generated abelian torsion-free group and K is a finite group of order k, say. It follows that $Z(S)^{(k)} = Y^{(k)} =_{def} H$ is a torsion-free abelian subgroup of finite index in S and H is normal in G. Hence S/H is a finite subgroup of G/H and since G/S is an elementary abelian 2-group, it follows by Lemma 3.1 that G/H is a periodic FC-group. In particular, so is $C_G(H)/H$ and by [12, Vol.I, p.122] $C_G(H)$ is an FC-group. Moreover, $G/C_G(H)$ is an elementary abelian 2-group as $S \leq C_G(H)$. Let $g \in G - C_G(H)$ and consider $H\langle g\rangle$. By Lemma 3.4 we have $y^g = y^{-1}$ for all $y \in H$ and hence $|G : C_G(H)| \leq 2$. Since G is not an FC-group, it follows that $C_G(H) = F$ and $|G : F| = 2$. ∎

By Proposition 5.1 $G = F\langle x\rangle$, where $x \in G$ satisfying $x^2 \in F$.

Next we propose to show that $F^{(2)}$ is of infinite order. Suppose that $E =_{def} F^{(2)}$ is of finite order. Consider $H =_{def} G/E$ and denote F/E by K. Since K is an elementary abelian 2-group, it follows by Lemma 3.5 that there exists a finite subgroup C of K which is normal in H such that x centralizes K/C. It follows that H/C is abelian and hence $H' \leq C$. But C and E are of finite order, so G' is also of finite order and consequently G is an FC-group, a contradiction.

So F is an FC-group and $F^{(2)}$ is of infinite order. It follows by Theorem A that $|F : Z(F)|$ is finite. Denote $Z(F) = Z$ and define:

(1) $$I = \{z \in Z | z^x = z^{-1}\} \text{ and}$$

(2) $$C = \{z \in Z | z^x = z\}.$$

Clearly I and C are normal subgroups of G.

Suppose that $|Z : C|$ is finite. Then $|G : C|$ is finite and hence, since $C \leq Z(G)$, G is an FC-group , a contradiction.

Suppose that $|Z : I|$ is finite. Then $|G : I|$ is finite and in particular $|J : I|$ is finite, where $J =_{def} C_G(I)$. It follows that J is an FC-group and since $F \leq J$ we conclude, in view of Proposition 5.1, that $J = F$ and G is nearly-dihedral, as claimed.

So we may assume that both $|Z : C|$ and $|Z : I|$ are infinite. Suppose that also $|Z : CI|$ is infinite and let $a_1, a_2, \ldots$ be representatives of distint cosets of CI in Z. Define $e_i = a_i x^{-1}$ for $i = 1, 2, \ldots$. If $e_i^2 = e_j^2$ for some $i \neq j$ then $a_i a_i^x = a_j a_j^x$ and $a_i a_j^{-1} = (a_j a_i^{-1})^x$, yielding $a_j a_i^{-1} \in I$, a contradition. Suppose now that $e_i e_j = e_j e_i$ for some $i \neq j$. Then $a_i a_j^x = a_j a_i^x$ and $a_i a_j^{-1} = (a_i a_j^{-1})^x$, yielding $a_i a_j^{-1} \in C$, a contradiction. Thus $e_i^2 \neq e_j^2$ and $e_i e_j \neq e_j e_i$ for $i \neq j$ and by Lemma 3.2 G does not belong to DS, a contradiction.

So we may assume that $|Z : C|$ and $|Z : I|$ are infinite, but $|Z : CI|$ is finite, which implies that both $|CI : I|$ and $|CI : C|$ are infinite. Let $c_1, c_2, \ldots$ be representatives of distinct cosets of I in CI which belong to C and let $e_1, e_2, \ldots$ be representatives of distinct cosets of C in CI which belong to I. Then $c_i^x = c_i$ for all i and since $c_i^{-1}c_j \notin I$ for $i \neq j$, we conclude that $c_i^{-1}c_j \neq c_ic_j^{-1}$, or $c_j^2 \neq c_i^2$ for $i \neq j$. Similarly, $e_i^x = e_i^{-1}$ for all i and since $e_i^{-1}e_j \notin C$ for $i \neq j$, we conclude that $e_ie_j^{-1} \neq e_i^{-1}e_j$, or $e_i^2 \neq e_j^2$ for $i \neq j$. Define now $f_i = c_ie_ix^{-1}$ for $i = 1, 2, \ldots$. If $f_i^2 = f_j^2$ for some $i \neq j$, then $c_ie_i(c_ie_i)^x = c_je_j(c_je_j)^x$ and $c_ie_ic_ie_i^{-1} = c_je_jc_je_j^{-1}$ yielding $c_i^2 = c_j^2$, a contradiction. Similarly, if $f_if_j = f_jf_i$ for some $i \neq j$, then $c_ie_i(c_je_j)^x = c_je_j(c_ie_i)^x$ and $c_ie_ic_je_j^{-1} = c_je_jc_ie_i^{-1}$, yielding $e_i^2 = e_j^2$, a contradiction. Thus $f_i^2 \neq f_j^2$ and $f_if_j \neq f_jf_i$ for $i \neq j$ and by Lemma 3.2 G does not belong to DS, a final contradiction.

6. Final Remarks

It follows from Theorems A and B that G belongs to DS if and only if either $|G^{(2)}|$ is finite, or $|G : Z(G)|$ is finite, or there exists a normal abelian subgroup H of G of finite index $|G : H|$, on which each element of $G - C_G(H)$ acts by conjugation as the inverting automorphism.

Suppose that G belongs to $DS(m)$ for some $m \geq 2$. What can we say about the above mentioned quantities? We claim that even for very small values of m, they are not bounded as a function of m. Indeed, if G is abelian then G belongs to $DS(2)$, but clearly $|G^{(2)}|$ can be infinite. If $G = D_\infty$, the infinite dihedral group and C_∞ denotes its cyclic subgroup of index 2, then G belongs to $DS(3)$, but $|G : Z(G)|$ is infinite. Moreover, G is nearly dihedral with respect to any $1 \neq H \leq C_\infty$ and hence $|G : H|$ is not bounded.

References

[1] L. Babai and V. T. Sós, *Sidon sets in groups and induced subgraphs of Cayley graphs,* Europ. J. Combinatorics **6** (1985), 101–114.

[2] Ja. G. Berkovich, G. A. Freiman and C. E. Praeger, *Small squaring and cubing properties for finite groups,* Bull. Austral. Math. Soc. **44** (1991), 429–450.

[3] B. J. Birch, R. G. Burns, S. O. Macdonald and P. M. Neumann, *On the orbit-sizes of permutation groups containing elements separating finite subsets,* Bull. Austral. Math. Soc. **14** (1976), 7–10.

[4] M. Cartwright, *The order of the derived group of a BFC-group,* J. London Math. Soc.(2) **30** (1984), 227–243.

[5] G. Freiman, *On two and three-element subsets of groups,* Aeq. Math. **22** (1981), 140–152.

[6] P. Longobardi and M. Maj, *The classification of groups with the small squaring property on 3-sets,* Bull. Austral. Math. Soc., to appear.

[7] B. H. Neumann, *Groups with finite classes of conjugate elements,* Proc. London Math. Soc.(3) **1** (1951), 178–187.

[8] B. H. Neumann, *Groups covered by permutable subsets,* J. London Math. Soc. **29** (1954), 236–248; Selected works of B. H. Neumann and Hanna Neumann, Vol. 5, pp. 940–953.

[9] B. H. Neumann, *A problem of Paul Erdős on groups,* J. Austral. Math. Soc., **21** (1976), 467–472; Selected works of B. H. Neumann and Hanna Neumann, Vol 5, pp. 1003–1008.

[10] P. M. Neumann, *A combinatorial problem in group theory,* Private communication.

[11] P. M. Neumann and M. R. Vaughan-Lee, *An essay on BFC-groups,* Proc. London Math. Soc.(3) **35** (1977), 213–237.

[12] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups* (2 Volumes), Springer-Verlag, New York, Heidelberg, Berlin, 1972.

[13] D. J. S. Robinson, *A Course in the Theory of Groups,* Graduate Texts in Mathematics, Vol.80, Springer-Verlag, New York, Heidelberg, Berlin, 1982.

[14] M. J. Tomkinson, *FC-groups,* Pitman, 1984.