Counting Squares of n-Subsets in Finite Groups

Mariagrazia Bianchi and Anna Gillio *
Dipartimento di Matematica
"F. Enriques"
Via Saldini 50
20133 Milano
Italy

Libero Verardi
Dipartimento di Matematica
Piazza di Porta San Donato 5
40127 Bologna
Italy

ABSTRACT. Let G be a finite group of order $n \geq 2$, $(x_1, \ldots, x_n)$ an n-tuple of elements of G and $A = (a_{ij})$ a square matrix of order n such that $a_{ij} = x_i x_j$. We investigate how many different types of such matrices could exist for $n = 2, 3$ and we deal with some of their properties. We show that for every group G the number of the ordered n-tuples corresponding to the same matrix is a multiple of $|G|$.

Introduction

Let G be a group and $(x_1, x_2, \ldots, x_n)$ an n-tuple of elements of G, $n > 1$. Let $A = (a_{ij})$ be a square matrix of order n such that $a_{ij} = x_i x_j$.

Of course if $|G| < \infty$ and $x_i \neq x_j \;\; \forall i \neq j$, A is a diagonal submatrix of the composition table of G.

The investigation of how many different types of such matrices could exist and of their properties, were problems solved by Freiman ([Fr]) for $n = 2, 3$. Then Brailovsky and Herzog [BH] have examined the case $n = 2$, showing that the number p_i of ordered couples of elements of G corresponding to

*Research partially supported by G.N.S.A.G.A. of C.N.R. and M.U.R.S.T. of Italy.

the matrix A is a multiple of $|G|$ and determining, for all i, the properties of those groups for which $p_i = 0$.

The aim of this paper is to extend these results and properties to the case $n \geq 3$.

In the first chapter we prove the following result:

Theorem A. *For every finite group G and for all $n \geq 2$, the number of ordered n-tuples associated to the same matrix is always a multiple of $|G|$.*

Our proof is independent of the one in [BH], related to the case $n = 2$.

Then we examine the case $n = 3$ and in the second chapter, using techniques different from Freiman's ones, we describe the 51 types of matrices related to products of three distinct elements of a group. For each of them we give the minimum order of those groups in which a certain matrix can occur.

The remaining two chapters are devoted to the classification of those groups in which the associated matrices have some peculiarities. We prove:

Theorem B. *If G is a finite group, then $p_i > 0$ for only one i if and only if G is cyclic of order 3, 4, or 5 or an elementary abelian 2-group.*

Theorem C. *If G is a group whose matrices have always at least two equal elements, then G is soluble. In particular, if $|G|$ is odd, then G is abelian, while if $|G|$ is even, then G has a normal abelian 2-Hall complement.*

1 Theorem A: Proof

Let A be a square matrix of order n, whose elements belong to the set $Q = \{1, 2, \ldots, n^2\}$. Let us associate to A a vector $v_A = (v_1, \ldots, v_{n^2})$ such that for $i, j \in \{1, 2, \ldots, n\}$ it is $v_h = a_{ij}$ where $h = n(i-1) + j$.

Now let m_A be a function defined by setting

$$m_A(h) = \max\{v_k \mid k \leq h\} \; \forall h \in \{1, 2, \ldots, n^2\}.$$

The matrix A is said to be *canonical*, if the following requirements are satisfied:

a) the elements of A belong to the set $\{1, 2, \ldots, n^2\}$;

b) $a_{11} = 1$;

c) the function $m = m_A$ has the following property

$$m(h+1) \leq m(h) + 1 \; \forall h = 1, 2, \ldots, n^2 - 1.$$

Given a square matrix M of order n, we can associate to it one and only one *canonical matrix* A by substituting its elements m_{ij} with the numbers of the set $\{1,\dots,n^2\}$ in such a way that conditions a) – c) are satisfied and that equal numbers correspond to equal elements of M and only to such.

Let now G be a group and $n \in N$, $n > 1$. Let $X = (x_1, x_2, \dots, x_n)$, where $x_1,\dots,x_n$ are elements of G and let A be the canonical matrix corresponding to the composition table of X. Such an A will be referred to as the *group-matrix of order n* corresponding to X. By $p_A(G)$ we will denote the number of different ordered n-tuples X of elements of G corresponding to A. It is immediate to prove that two n-tuples $(x_1, x_2, \dots, x_n)$ and $(y_1, y_2, \dots, y_n)$ correspond to the same group-matrix if and only if for all i, j, r and s we have $x_ix_j = x_rx_s \Longleftrightarrow y_iy_j = y_ry_s$.

We will prove that if G is a finite group, then $p_A(G)$ is a multiple of $|G|$.

Let $[x,y] = x^{-1}y^{-1}xy$ for $x,y \in G$ and let

$$H_X = \{g \in G \mid [x_i, g] = [x_1, g] \text{ for all } i = 1, \dots n\}.$$

Of course, H_X is a subgroup of G. Now let

$$V_X = \{h \in H_X \mid [x_i, h] \in H_X,\ \forall i\}.$$

Then V_X is a subgroup of H_X.

Lemma 1.1. *Let G be a finite group, A one of the group-matrices of order n and $X = (x_1,\dots,x_n)$ an ordered n-tuple of elements of G corresponding to A. Let $H = H_X$, $V = V_X$ and T be a right transversal of H in G containing 1_G. Finally set:*

$$\Omega_X = \{(hx_1h')^t, \dots, (hx_nh')^t \mid h, h' \in H, t \in T\}.$$

Then:

a) *Each element of Ω_X corresponds to A.*

b) *Let $h, h' \in H$ and $t \in T$. Then the equation*

$$(x_1, \dots, x_n) = ((hx_1h')^t, \dots, (hx_nh')^t)$$

holds if and only if $t = 1_G$, $h \in V$ and $h' = x_i^{-1}h^{-1}x_i$ for all $i = 1, \dots, n$;

c) *Let $h_1, h_2, h_3, h_4 \in H$ and $t', t'' \in T$. Then the equation*

$$((h_1x_1h_2)^{t'}, \dots, (h_1x_nh_2)^{t'}) = ((h_3x_1h_4)^{t''}, \dots, (h_3x_nh_4)^{t''})$$

holds if and only if $t' = t''$ and there exists $v \in V$ such that $h_3 = h_1v$, $h_4 = x_i^{-1}v^{-1}x_ih_2$, for all $i = 1, \dots, n$.

d) $|\Omega_X| = |G|[H : V]$.

e) *If $Y = (y_1, \dots, y_n) \in \Omega_X$ then $\Omega_Y = \Omega_X$.*

Proof: a) For all $h, h' \in H$ and $t \in T$ the ordered n-tuple $((hx_1h')^t, \dots, (hx_nh')^t)$ corresponds to A. In fact, set $c = [x_k, h'h]$ for $k = 1, 2, \dots, n$. We get

$$h'hx_kh' = x_kh'hc^{-1}h'$$

and so

$$\begin{aligned} &(hx_ih')^t(hx_jh')^t = (hx_rh')^t(hx_sh')^t \iff \\ &t^{-1}hx_ih'hx_jh't = t^{-1}hx_rh'hx_sh't \iff \\ &hx_ix_jh'hc^{-1}h' = hx_rx_sh'hc^{-1}h' \iff x_ix_j = x_rx_s. \end{aligned}$$

It follows that the group-matrix corresponding to the new n-tuple is precisely A.

b) We have $x_i = (hx_ih')^t \iff x_i[x_i, t^{-1}] = x_i[x_i, h^{-1}]hh' \iff [x_i, t^{-1}] = [x_i, h^{-1}]hh'$ which is independent of i, since $h^{-1} \in H$. Thus $t \in H$, and so $T \cap H = \{1_G\} = 1$ implies $t = 1_G$. But then $x_i = hx_ih'$, $\forall i$, from which it follows immediately $[x_i, h] = h^{-1}h' \in H$ $\forall i$. So $h \in V$ and $h' = x_i^{-1}h^{-1}x_i$, $\forall i$.

c) Suppose $(h_1x_ih_2)^{t'} = (h_3x_ih_4)^{t''}$, $\forall i$. Then if $t't''^{-1} = ht$, $h \in H$, $t \in T$ we have $(h_1x_ih_2)^{ht} = h_3x_ih_4$, so $(h^{-1}h_1x_ih_2h)^t = h_3x_ih_4$.

Now let $c^{-1} = [x_i, h^{-1}h_1]$; since $h^{-1}h_1 \in H$, c is independent of i and for all i, $h^{-1}h_1x_ih_2h = x_ih^{-1}h_1ch_2h$. It follows:
$(x_ih^{-1}h_1ch_2h)^t = h_3x_ih_4$, so $x_i[x_i, t](h^{-1}h_1ch_2h)^t = x_i[x_i, h_3^{-1}]h_3h_4$, that is $[x_i, t] = [x_i, h_3^{-1}]h_3h_4(h^{-1}h_1ch_2h)^{-t}$, which is independent of i. So $t \in H$ and, as before, $t = 1_G$.

Therefore $tt''^{-1} \in H$ and, T being a transversal, we get $t' = t''$. We deduce that $h_1x_ih_2 = h_3x_ih_4$ and this implies that $x_i = (h_1^{-1}h_3)x_i(h_4h_2^{-1})$ $\forall i$.

Applying b) we get $h_1^{-1}h_3 = v \in V$ and $(h_4h_2^{-1}) = x_i^{-1}v^{-1}x_i$. It follows $h_3 = h_1v$, $h_4 = x_i^{-1}v^{-1}x_ih_2$, $\forall i$.

Vice versa, if $t' = t''$ and there exists $v \in V$ such that $h_3 = h_1v$, $h_4 = x_i^{-1}v^{-1}x_ih_2$, $\forall i$, then the n-tuples are equal.

d) From c) it follows that in $H \times H \times T$ the equivalence relation $\mathcal{R}$

$$(h_1, h_2, t')\mathcal{R}(h_3, h_4, t'') \iff (h_1x_ih_2)^{t'} = (h_3x_ih_4)^{t''}, \ \forall i = 1, \dots, n$$

has equivalence classes containing $|V|$ elements.

This means that:

$$|\Omega_X| = |\frac{H \times H \times T}{\mathcal{R}}| = \frac{|H|^2[G\colon H]}{|V|} = |G|[H\colon V],$$

so $|\Omega_X| = |G|[H\colon V]$.

e) We prove that, if $Y \in \Omega_X$ then $\Omega_Y \subseteq \Omega_X$ and $|\Omega_Y| = |\Omega_X|$.

First of all, let $u, v \in G$ such that $c = [x_i u, v]$ is constant with respect to i. Then $c = [x_i, v]^u [u, v]$ and so $[x_i, v] = (c[u, v]^{-1})^{u^{-1}}$ is independent of i and this implies that v is in H.

Vice versa for all $u \in G$, $v \in H$ the commutator $[x_i u, v]$ is independent of i.

Now let $Y \in \Omega_X$: we have $y_i = (hx_i h')^t$ with $h, h' \in H$ and $t \in T$, $i = 1, \dots, n$. Let $k \in G$ be such that $d = [y_i, k]$ is independent of i. If d' and k' are elements of G such that $d = (d')^t$ and $k = (k')^t$, it follows that $d = (d')^t = [(hx_i h')^t, (k')^t]$, so $d' = [hx_i h', k']$. But $h \in H$ and we can write $hx_i = x_i hc$, with c independent of i, and from what we have proved, it follows $k' \in H$, that is $k \in H^t$. Therefore $H_Y \subseteq H^t$. A similar argument shows that $H^t \subseteq H_Y$ and then $H_Y = H^t$, and T^t is one of its right transversals.

Now consider the n-tuple $((ky_1 k')^u, \dots, (ky_n k')^u) \in \Omega_Y$. As $k, k' \in H^t$ we can suppose $u \in T^t$. Then $k = t^{-1} h_0 t$ and $k' = t^{-1} h'_0 t$ with $h_0, h'_0 \in H$ and $u = t^{-1} t' t$ for $t' \in T$.

Finally we get

$$(ky_i k')^u = (h_0^t (hx_i h')^t (h'_0)^t)^u = (h_0 hx_i h' h'_0)^{tu} = (h_0 hx_i h' h'_0)^{t't}.$$

As before, there exist $h'' \in H$ and $t'' \in T$ such that $t't = h''t''$ and then $(h_0 hx_i h' h'_0)^{t't} = (h_0 hx_i h' h'_0)^{h''t''} = ((h''^{-1} h_0 h) x_i (h' h'_0 h''))^{t''}$ is a component of an element in Ω_X.

It follows $\Omega_Y \subseteq \Omega_X$.

Now, we compute $|\Omega_Y|$. Because of d) it is necessary and sufficient to compute $|V_Y|$, where $V_Y = \{k \in H_Y \mid [y_i, k] \in H_Y\}$. We have $H_Y = H^t$, $k = h_0^t$ for a suitable $h_0 \in H$, so $[y_i, k] = [(hx_i h')^t, h_0^t] = [hx_i h', h_0]^t \in H^t \iff [hx_i h', h_0] \in H \iff [hx_i, h_0]^{h'} [h', h_0] \in H \iff [hx_i, h_0] \in H \iff [hx_i, h_0]^h \in H \iff [x_i h, h_0^h] \in H \iff [x_i, h_0^h]^h [h, h_0]^h \in H \iff [x_i, h_0^h] \in H \iff h_0^h \in V \iff h_0 \in hVh^{-1} \iff k \in (hVh^{-1})^t$.

But then $V_Y = (V^{h^{-1}})^t$ has the same order as V.

Therefore $|\Omega_Y| = |G|[H^t : (V^{h^{-1}})^t] = |G|[H : V] = |\Omega_X|$.

Now, in view of $\Omega_Y \subseteq \Omega_X$, it follows that $\Omega_Y = \Omega_X$.

Theorem A. *For each group matrix A of order n, the number $p_A(G)$ of ordered n-tuples $X = (x_1, \dots, x_n)$ of elements of G, associated to the matrix A, is a multiple of $|G|$.*

Proof: Let U_A be the set of the ordered n-tuples X associated to A. For each $X \in U_A$, by the previous Lemma 1.1 a), Ω_X a subset of U_A.

Besides, from 1.1.e), it follows that if $X, Y \in U_A$ and $Z \in \Omega_X \cap \Omega_Y$ then $\Omega_X = \Omega_Y = \Omega_Z$.

We obtain in this way a partition of U_A and, as $|G|$ divides $|\Omega_X|$, we get that $|G|$ divides $p_A = |U_A|$.

2 The case $n = 3$

Let A be a square matrix of order 3, whose elements belong to the set $Q = \{1, 2, \dots, 9\}$ satisfying the conditions a), b), c) of the previous chapter. Besides, we require the following condition:

d) no element can be repeated in each row and column of A.

We observe that condition c) implies

$$m(h+j) \leq m(h) + j, \ \forall j = 1, \dots, 9-h,$$

so

$$v_{h+j} \leq m(h) + j.$$

Every such matrix A can be represented by the number $n(A)$ with 9 digits, which is obtained by writing consecutively the 9 elements of the vector v_A. We define $n(A)$ as the *representative number* (or *schema*) of A. A suitable algorithm shows the existence of 588 matrices which satisfy conditions a) – d).

Given a square matrix M of order 3 corresponding to an ordered triplet (x, y, z) of different elements of a group G, we can associate one and only one canonical matrix A by substituting its elements m_{ij} with the numbers of the set $\{1, 2, \dots, 9\}$ in such a way that conditions a) – d) are satisfied and that equal numbers correspond to equal elements and only to such.

The matrix A is necessarily one of the 588 mentioned above.

Example: Let $G = S_3$, $a = (1, 2)$, $b = (1, 2, 3)$. Denoting by i the identity, the multiplication table M of the triplet (b, b^2, a) and its canonical matrix A are:

$$M = \begin{pmatrix} b^2 & i & ab^2 \\ i & b & ab \\ ab & ab^2 & i \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 5 & 3 & 2 \end{pmatrix}$$

$v_A = (1, 2, 3, 2, 4, 5, 5, 3, 2)$ and $n(A) = 123245532$.

In general, if we permute the 3 elements x, y, z of G, we produce at most 6 different canonical matrices, which can be obtained from A in the following way: if $\alpha \in S_3$ and $A = (a_{ij})$, put $A' = (a_{\alpha(i),\alpha(j)})$, $i, j = 1, 2, 3$. Then we give the canonical form to A' and get A^α. So if A corresponds to the ordered triplet (x_1, x_2, x_3) of different elements of G, A^α corresponds to the triplet $(x_{\alpha(1)}, x_{\alpha(2)}, x_{\alpha(3)})$. Following Freiman's notation we call A^α *isomorphic* to A. As representative of the set $\{A^\alpha \mid \alpha \in S_3\}$ we can choose that matrix whose representative number is the minimum and we call it the *normalized canonical matrix.*

With a suitable selection we can find 125 normalized canonical matrices and by elimination of those not derived from groups, we get 51 matrices, among which 6 are symmetric and 45 are not. Freiman himself gives for each of them a triplet of elements of a group from which the matrix derives.

Matrices A_λ, $\lambda = 1, 2, \ldots, 51$, are the so-called *group-matrices*: they are described in the following list using their representative schemas, and they are divided into 7 sections according to the number, from 3 to 9, of distinct elements. The list has a double enumeration: the first one from 1 to 51, the second denotes the place occupied by the schema in Freiman's list (see the following Remark). For each matrix we also give a group of minimal order containing a triplet with which the matrix is associated. We use the following symbols:

$h\colon k_n$ denotes the group of order kh whose presentation is the following:

$$< a, b \mid a^h = b^k = 1, a^b = a^n >,$$

Z_n and D_{2n} denote respectively the cyclic group of order n and the dihedral group with $2n$ elements.

The matrices with an $\star$ are symmetric.

These data are obtained by examining one by one the groups of small order with a computer. In particular we found that 24 is the minimum order of an abelian group ($C_6 \times C_4$) in which all the 6 symmetric matrices appear and we reach the same result from a theoretical point of wiew in chapter 3.

Remark: All groups in the following list have transitive representations of degree less or equal 8, with the exception of $11\colon 5_3$ which has a representation of degree 11. Considering the fact that if a matrix A_λ appears in a subgroup, it appears of course in the group too, we can state that in $S_8 \times (11\colon 5_3)$ we can construct all the 51 matrices (remark: $S_8 \times (11\colon 5_3)$ has order $8!55 = 2,217,600$).

1*	(4*)	123231312	Z_3	27	(370)	123435614	$7\colon 3_2$
2	(105)	123312231	S_3				
				28	(18)	123214567	D_{12}
3*	(1*)	123214341	E_{2^2}	29	(67)	123245367	A_4
4*	(2*)	123214342	Z_8	30	(89)	123245567	$5\colon 4_2$
5	(4)	123214431	D_8	31	(101)	123245671	$8\colon 2_3$
6	(5)	123214432	D_8	32	(102)	123245672	A_4
7	(142)	123341432	A_4	33	(154)	123341567	$5\colon 4_2$
				34	(175)	123342567	$7\colon 3_2$
8*	(3*)	123214345	Z_6	35	(186)	123345267	A_4
9	(1)	123214351	S_3	36	(197)	123345467	$11\colon 5_3$
10	(6)	123214351	$8\colon 2_5$	37	(208)	123345567	$7\colon 3_2$
11*	(8*)	123234345	Z_5	38	(211)	123345617	S_4
12	(83)	123245532	S_3	39	(215)	123345637	S_4
13	(117)	123314251	D_{10}	40	(221)	123345672	$11\colon 5_3$
14	(163)	123342415	$5\colon 4_2$	41	(222)	123345674	$3\colon 4_2$
15	(198)	123345512	$5\colon 4_2$	42	(289)	123415671	Q_8
				43	(290)	123415672	$3\colon 4_2$
16	(3)	123214356	S_3	44	(313)	123431567	$7\colon 6_3, 9 : 3_4$
17	(9)	123214456	A_4	45	(371)	123435617	A_4
18	(16)	123214561	D_{12}	46	(380)	123435672	$9\colon 3_4, 7 : 6_3$
19	(17)	123214562	$8\colon 2_3$				
20*	(15*)	123245356	Z_7	47	(104)	123245678	D_{10}
21	(66)	123245364	Q_8	48	(223)	123345678	A_4
22	(85)	123245536	$3\colon 4_2$	49	(292)	123415678	D_8
23	(153)	123341564	S_3	50	(382)	123435678	$S_3 \times Z_3$
24	(185)	123345264	$8\colon 2_3$				
25	(196)	123345462	$SL_2(3)$	51	(573)	123456789	A_4
26	(210)	123345614	$8\colon 23$				

Together with the 51 matrices corresponding to triplets of different elements, we can consider those corresponding to triplets of either partially or totally equal elements. In a canonical way we obtain 5 matrices, whose representative schemas are:

a) 111 111 111

b) 112 112 221

c) 112 112 223

d) 112 112 331

e) 112 112 334

We observe that a) corresponds to the case of 3 equal elements, b), c), d), e) correspond to the case of only two equal elements. These 5 matrices are in bijection with those of order 2 derived from couples of elements of a group, studied in [BH]. We denote those matrices by B_0, B_1, B_2, B_3 and B_4.

Remark: 1. In the sequel we will denote by p_i, $i = 1, \dots, 51$, the number of triplets of the group G corresponding to a group-matrix isomorphic to the matrix A_i.

2. As in [BH] we can try to compute the number u of the ordered triplets (a, b, c) of elements of G (distinct or not) but with the same square: $a^2 = b^2 = c^2$. The corresponding matrices A_λ are those with $\lambda \in V = \{2, 3, 5, 9, 13, 18, 42\}$ and also B_0, B_1, B_3.

For each $x, y \in G$ we define an equivalence relation by setting $x \sim y \iff x^2 = y^2$. Let $[a_1], \dots, [a_s]$ be the equivalence classes and let $\theta_2(a_i^2) = |[a_i]|$.

In the triplet (a, b, c) we have $b \sim c \sim a$, so from each class $[a_i]$ we get $(\theta_2(a_i^2))^3$ triplets and in all

$$u = \sum_{i=1}^{s} \theta_2(a_i^2)^3.$$

Now, there are $|G|$ triplets of type (a, a, a); besides from [BH] with trivial arguments it follows that the number of triplet (a, a, b) corresponding to B_1 is $3k_2|G|$, where k_2 is the number of conjugacy classes of involutions, while the number of matrices of type B_3 is $3(k_r - 1 - k_2)|G|$ where k_r is the number of real characters. In all we get $(3k_r - 2)|G|$ triplets corresponding to matrices of type B_0, B_1, B_3.

If we compute the number of matrices of type A_λ, $\lambda \in V$ we obtain:

$$\sum_{\lambda \in V} p_\lambda = \sum_{i=1}^{s} \theta_2(a_i^2)(\theta_2(a_i^2) - 1)(\theta_2(a_i^2) - 2)$$

and so

$$\sum_{\lambda \in V} p_\lambda = u - (3k_r - 2)|G|.$$

Notice that if $o(x)$ is odd, it is $x^2 = y^2 \iff y = x$, so the class $[x]$ cannot provide a triplet of distinct elements. Then the sum is extended over those classes containing elements of even order.

In any case, while $\sum_{i=1}^{s}(\theta_2(a_i^2))^2 = k_r|G|$, (see [BH]), it seems not easy to determine a formula for u using characters.

3 Groups with special types of group-matrices

We will characterize those groups for which either only some of the 51 matrices, corresponding to triplets of distinct elements, appear or some of them are missing.

Proposition 3.1. *Let G be a group with $|G| > 2$. Then:*

a) *G is abelian if and only if $p_i > 0$ only for $i \in \{1, 3, 4, 8, 11, 20\}$.*

b) *If G is finite, then $|G|$ is even if and only if $p_i > 0$ for some $i \in \{2, 3, 4, 5, 6, 8, 9, 10, 13, 16, 17, 18, 19, 21, 23, 24, 26, 28, 31, 41, 42, 43, 49\}$ (on the principal diagonal one can always find at least 2 equal elements).*

c) *If G is finite, then it is abelian of odd order if and only if $p_i = 0$ for all $i \notin \{1, 11, 20\}$.*

Proof: a) If the 3 elements commute, the multiplication table is symmetric and the matrix A_i too. Analyzing the list, we discover that the symmetric matrices are only those corresponding to numbers 1, 3, 4, 8, 11, 20. Vice versa, if the matrices corresponding to triplets of distinct elements of G are isomorphic to those 6 only, then G is abelian.

b) If $|G|$ is even, there exists $u \in G$ such that $u^2 = 1_G = 1_G^2$. Therefore if $v \in G$ is another element, the matrix A_i corresponding to the triplet $\{1_G, u, v\}$ has at least two equal elements on the principal diagonal.

Vice versa if one of the matrices of G has two equal elements on its diagonal, then we can find in G two elements x, y, $x \neq y$ such that $x^2 = y^2$. If $|G|$ were odd, then $x = y$, a contradiction. So $|G|$ is even. Examining the list, we find 23 matrices with at least 2 equal elements on the diagonal, those appearing in the statement of this proposition.

It follows that $|G|$ is odd if and only if none of its matrices is of these types.

c) follows from a) and b).

Lemma 3.2. *If G is a group, but not an elementary abelian 2-group, then $p_1 + p_4 + p_{11} > 0$.*

Proof: Let G be a group and consider the cyclic subgroup $\langle a \rangle$, where $o(a) > 2$. Let $x = a^i$, $y = a^j$, $z = a^h$ be distinct elements. Their multiplication table is

$$\begin{pmatrix} a^{2i} & a^{i+j} & a^{i+h} \\ a^{i+j} & a^{2j} & a^{j+h} \\ a^{i+h} & a^{j+h} & a^{2h} \end{pmatrix}$$

and it is symmetric. If we consider the triplet $\{1 = 1_G, a, a^{-1}\}$ the corresponding matrix is symmetric of type:

$$\begin{pmatrix} 1 & a & a^{-1} \\ a & a^2 & 1 \\ a^{-1} & 1 & a^{-2} \end{pmatrix}$$

that is, according to the previous notation:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & \alpha & 1 \\ 3 & 1 & \beta \end{pmatrix}$$

with $\alpha \in \{3,4\}$ and $\beta \in \{2,4,5\}$ (but if $\alpha = 3$ then $\beta \neq 5$).

Examining the 6 symmetric matrices we get that only 3 of them are of this type and precisely: A_1, A_4 and A_{11}. This means that at least one of them appears among the matrices of G, so $p_1 + p_4 + p_{11} > 0$.

Remark: By Theorem 3.5 this result is the best possible.

Lemma 3.3. *Let G be a group with $|G| > 2$.*

a) *if $p_1 > 0$ then G possesses a subgroup of order 3,*

b) *if $p_3 > 0$ then G possesses an elementary abelian subgroup of order 4,*

c) *if $p_4 > 0$ then G possesses a cyclic subgroup of order 4.*

Proof: a) Let $p_1 > 0$ and let x, y, z be 3 distinct elements of G corresponding to the matrix $A_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$.

It is easy to verify that the 3 elements commute, and $x^3 = y^3 = z^3$. Thus $(xy^{-1})^3 = 1_G$, so G possesses a subgroup P of order 3.

b) Let $p_3 > 0$ and x, y, z be distinct elements of G associated to the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \\ 3 & 4 & 1 \end{pmatrix}$. They commute and $x^2 = y^2 = z^2$, so G has an elementary abelian subgroup of order 4 which is generated by $\{xy^{-1}, xz^{-1}\}$.

c) Let $p_4 > 0$ and x, y, z be distinct elements of G associated to the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \\ 3 & 4 & 2 \end{pmatrix}$.

They commute and $x^2 = y^2$, $z^2 = xy$, so $z^4 = (xy)^2 = x^4$.

It follows $(xz^{-1})^4 = 1$, and since $x^2 \neq z^2$, G possesses a cyclic subgroup of order 4.

Corollary 3.4. *$Z_6 \times Z_4$ is the abelian group of minimal order which possesses all the 6 symmetric matrices.*

Proof: As $p_1 > 0$, it follows that G has an element of order 3 and, as $p_3 > 0$, G possesses an elementary abelian subgroup of order 4, so $|G| \geq 12$; $p_4 > 0$ implies the existence of an element of order 4, so $|G| \geq 24$. Thus the group $G = Z_6 \times Z_4$ is minimal with the required property as $|G| = 24$ and

$$p_1 = 24, p_3 = 144, p_4 = 288, p_8 = 4032, p_{11} = 504, p_{20} = 6624.$$

The following theorem characterizes those groups for which there exists one and only one i such that $p_i > 0$.

Theorem 3.5 (Theorem B). *Let G be a finite group such that $|G| > 2$. If $p_i > 0$ for only one i, then $i \in \{1, 3, 4, 11\}$. Besides:*

a) $i = 3 \Longleftrightarrow G$ *is an elementary abelian 2-group.*

b) $i = 1 \Longleftrightarrow G$ *is cyclic of order 3.*

c) $i = 4 \Longleftrightarrow G$ *is cyclic of order 4.*

d) $i = 11 \Longleftrightarrow G$ *is cyclic of order 5.*

Proof: If G is an elementary abelian 2-group, then $x^2 = 1$ for all $x \in G$, so its matrices are not only symmetric but they have 3 equal elements on the diagonal. But there is only one matrix with these features and it is equivalent to itself. So all matrices of G coincide with A_3. Now Lemma 3.2 assures that the only other possibilities are A_1, A_4 and A_{11}. Having established this, we argue as follows:

a) We have already proved that if G is an elementary abelian 2-group, we get only $p_3 > 0$. Vice versa, if in a group G all matrices are isomorphic to A_3, then $x^2 = 1_G^2 = 1_G$, $\forall x \in G$, so G is elementary abelian.

b) If $G \simeq Z_3$, then $p_1 = 1$ and $p_i = 0$ for $i > 1$. Vice versa, let G be a group such that $p_i = 0$ for all $i \neq 1$. Proposition 3.1 and Lemma 3.3 assure that G is abelian of odd order and it possesses an element a of order 3. Let $x = 1_G$ and $y = a$; for every z we must have $yz = 1_G$, so $z \in \langle y \rangle$. It follows $G = \langle a \rangle$, cyclic of order 3.

c) If $G \simeq Z_4$ then $p_4 \neq 0$ and $p_i = 0$ for $i \neq 4$. Vice versa, let G be a group such that $p_i = 0$ for $i \neq 4$; then G is abelian and it possesses an element a of order 4. If $x = 1_G$ and $z = a$, then for all $y \in G$ it is either $y^2 = x^2 (= 1_G)$ or $y^2 = z^2$. In the first case we get either $y = 1_G$ or

$y = xy = z^2$ and in the second case we get $yz = x^2 = 1_G$. In both cases $y \in \langle z \rangle$ and consequently $G = \langle z \rangle$ is cyclic of order 4.

d) If $G \simeq Z_5$ then $p_{11} \neq 0$ and $p_i = 0$ for $i \neq 11$. Vice versa, let G be a group such that $p_i = 0$ for $i \neq 11$. First of all G is an abelian group of odd order. Let a be a non-trivial element of G, with $o(a) = p$, p prime. Because of a), b), c), it is $p \geq 5$. If it were $p > 5$, putting $x = a$, $y = a^2$, $z = a^4$, the corresponding matrix would be of type A_{20}, a contradiction; so necessarily G is an abelian 5-group. On the other hand set $x = 1_G$ and $y = a$; then $z = 1_G z = xz = y^2$, $\forall z \in G$, so $z \in \langle y^2 \rangle = \langle y \rangle$. It follows that $G = \langle y \rangle \cong Z_5$.

Remark: The matrix A_3 does not characterize a triplet of elements of order 2 which commute. In fact, let $G = \langle a, b \mid a^4 = b^2 = 1_G = [a, b] \rangle \simeq Z_4 \times Z_2$; the triplet $\{a, a^3, ab\}$ corresponds to the matrix A_3, the 3 elements commute and they have the same squares.

Proposition 3.6. *Let p be a prime > 3 and G be a group of order p. Then $p_{11} = 6\binom{p}{2}$, $p_{20} = 6\binom{p}{3} - 6\binom{p}{2}$, and $p_i = 0$ $\forall i \neq 11, 20$.*

Proof: Because of Lemmas 3.1 c) and 3.3 a), necessarily $p_i = 0$ for all $i \neq 11, 20$. Now let a be a generator of G and let (a^i, a^j, a^k) be a triplet of distinct elements of G. The matrix A_{11} corresponds to them if and only if $i + j \equiv 2k \pmod{p}$. It follows $i \equiv 2k - j \pmod{p}$, so there exist $p(p-1)$ solutions $\pmod{p}$ with different elements. Exchanging k with i and with j we obtain that the number of these matrices is $3p(p-1)$, as required. Since the total number of triplets is $6\binom{p}{3}$, the conclusion follows.

Remark: It can be shown that for the two non isomorphic groups of order 25 we have $p_{11} = 1800$ and $p_{20} = 12000$. Hence the list of matrices does not characterize a group.

4 On the matrix A_{51}

Now let us examine the matrix A_{51}, whose 9 elements are all different: of course if there exists a subgroup $H \leq G$ such that $p_{51}(H) \neq 0$ then $p_{51}(G) \neq 0$.

But also if there exists $N \lhd G$ such that $p_{51}(G/N) \neq 0$ then $p_{51}(G) \neq 0$.

In fact, given 3 elements $x_i \in G$, $i = 1, 2, 3$ such that $(x_i N)(x_j N) \neq (x_r N)(x_s N)$, we must have $x_i x_j \neq x_r x_s$. This is not true for the other matrices. For example $p_3(Q_{16}) = 0$, while $p_3(Q_{16}/Z(Q_{16})) = p_3(D_8) \neq 0$.

Remark: The alternating group A_4 is the smallest group G such that $p_{51}(G) \neq 0$ (see for example the triplet $\{(1,2,3), (2,3,4), (1,4)(2,3)\}$).

We deduce that for every group G involving A_4 it is $p_{51} \neq 0$.

Theorem 4.1. *If G is a finite group such that $p_{51}(G) = 0$, then G is soluble.*

Proof: Deny and suppose that G is non-soluble. So G possesses two subgroups H and K such that $K \triangleleft H$ and H/K is a non abelian simple group. By previous remark it is sufficient to prove the statement for every simple group, in particular for all minimal simple groups, which are (see [Hu I])

(a) $PSL_2(2^p)$, p prime;

(b) $PSL_2(3^p)$, p prime;

(c) $PSL_2(p)$, p prime, $p > 3$, $p^2 + 1 \equiv 0 \pmod 5$;

(d) $PSL_3(3)$;

(e) $Sz(2^p)$, p an odd prime.

We will examine each case separately:

(a) Dickson's theorem (see [Hu I]) assures that a Sylow 2-subgroup V of $PSL_2(2^p)$ is elementary abelian of order 2^p. Besides the group $PSL_2(2^p)$ contains the semidirect product of V by a cyclic subgroup T of order $2^p - 1$, which acts transitively on the subgroups of order 2 of V. Say x is a generator of T, we can find a suitable basis $\{a_1, a_2, \dots, a_p\}$ of V such that

$$a_i^x = a_{i+1}, i = 1, \dots, p-1, a_p^x = a_1 a_2^{h_2} \dots a_p^{h_p}, h_i \in \{0, 1\}.$$

Then, for all $i > 1$, it is $xa_i = a_{i-1}x$ and besides $xa_1 = wx$, where $w = a_1^{h_2} \dots a_{p-1}^{h_p} a_p$. It follows that $w \in V$, $1_G \neq w \neq a_1$, so we get also $a_1 w \neq 1_G$. Besides $x^2 \neq 1_G$ and $x \notin V$. So the triplet $(a_1, x, a_1 x)$ corresponds to the matrix A_{51}.

(b), (c) Because of Dickson's theorem, these groups contain the alternating group A_4, so $p_{51} \neq 0$.

(d) A Sylow 2-subgroup of $PSL_3(3)$ is isomorphic to the following group (see [Hu I]):

$$\langle a, b \mid a^8 = b^2 = 1, a^b = a^3 \rangle$$

for which the triplet $\{a, b, ab\}$ corresponds to the matrix A_{51}.

(e) The group $Sz(2^p)$, $q = 2m+1$, has a cyclic subgroup U of order $2^q + 2^{m+1} + 1$ (see [Hu III] p. 190) whose normalizer N has order $4(2^q + 2^{m+1} + 1)$ and N/U is cyclic. Say u is a generator of U, there exists $t \in N$ such that $o(t) = 4$ and $u^t = u^q$. The elements u, u^2, u^q, u^{q+1} are all distinct and the same holds for 1_G, $t^{-1} = t^3$, t^2 which do not belong to U. As $N = [U]\langle t \rangle$, the elements of the form $u^h t^k$ are all distinct for $h \in \{0, 1, \dots, 2^q + 2^{m+1}\}$ and $k \in \{0, 1, 2, 3\}$. Then A_{51} is the matrix corresponding to the triplet $\{u, t^{-1}, ut^{-1}\}$. This holds in particular if $q = p$ is an odd prime.

Concluding, for all minimal simple groups it is $p_{51} \neq 0$ and the same holds for all non-soluble groups.

Lemma 4.2. *Let G be a finite group such that $p_{51}(G) = 0$. Then*

a) *if G is a p-group, with p an odd prime, then G is abelian;*

b) *for all odd prime divisors p of $|G|$, the Sylow p-subgroups of G are abelian.*

Proof: a) Let G be a non-abelian p-group and let $a, b \in G$ such that $[a,b] \neq 1_G$ and $H = \langle a, b \rangle$. Let us consider the quotient $P = H/\Gamma_3(H)$. Then P is nilpotent of class 2 and it is generated by 2 elements, which we denote also by a and b. The triplet (a, b, ab) corresponds to the matrix A_{51}. In fact, if we put $z = [a,b]$, the 9 products are:

$$a^2, ab, a^2b; abz, b^2, ab^2z; a^2bz, ab^2, a^2b^2z.$$

As $|P|$ is odd and a and b generate P, we get neither $b \in \langle a, P' \rangle \leq \langle a, \Phi(P) \rangle$ nor $a \in \langle b, P' \rangle$. Consequently those 9 products are distinct and the corresponding matrix is A_{51}. But then $p_{51}(G) \neq 0$. Thus if $p_{51} = 0$, then G is abelian.

b) follows from a) as the property $p_{51} = 0$ is inherited by subgroups.

Now we state Theorem C, whose proof derives from the following Propositions 4.3 and 4.4.

Theorem C. *Let G be a finite group whose matrices have at least two equal elements. Then G is soluble. In particular if $|G|$ is odd, then G is abelian and if $|G|$ is even, then G has a normal abelian 2-Hall complement.*

Proposition 4.3. *Let G be a finite group such that $p_{51}(G) = 0$. If $|G|$ is odd, then G is abelian.*

Proof: By induction on $|G|$. Because of Lemma 4.2, it is sufficient to prove that all Sylow subgroups are normal in G.

Let P be a minimal normal subgroup of G. Because of the inductive hypotesis, G/P is abelian, so $G' \leq P$. If there is another minimal normal subgroup different from P, then G is abelian.

Now let us suppose that P is unique: as P is a p-subgroup, choose S a Sylow p-subgroup containing it (which is normal in G and abelian) and let M be a p-complement of S in G. If $P \neq S$, PM is abelian and, containing P, is normal in G. But in this case, every Sylow subgroup is normal in G. Now let $P = S$. If M is not a q-group, for a prime q, M is the product of two Hall subgroups M_1 and M_2: so $\forall i = 1, 2$ it is $G \neq PM_i \triangleleft G$, PM_i is abelian and each of its Sylow subgroups (and therefore every Sylow subgroup of G) is normal in G.

If M is a q-group, q prime, then PM^q is a normal and abelian subgroup, so $M^q \triangleleft G$. If $M^q \neq 1_G$, then M would contain a minimal normal subgroup different from P, a contradiction. It follows that $|M| = q$ and $|G| = p^\alpha q$.

Suppose that G is non-abelian and first of all let $\alpha > 1$. As P is minimal normal, if $x \in P$ and $y \in Q$, it is $x^y = x[x, y] \notin \langle x \rangle$. We easily verify that the triplet (y, x, yx) corresponds to the matrix A_{51}. In fact the 9 products are:

$$y^2, yx, y^2x; yxr, x^2, yx^2r; y^2xr, yx^2, y^2x^2r$$

where $r = [x, y]$ and $rx = xr$ as $r, x \in P$ elementary abelian, and they are all distinct. But this is in contradiction with the hypothesis on G. So it must be $\alpha = 1$ and $|G| = pq$ with $p > q$, $p > 3$; besides $p \equiv 1 \pmod q$ (if $p = 3$ then $|G| = 6$, a contradiction).

As before, suppose $x \in P$, $y \in M$: then $x^y = x^i$ where $q \pmod p$ is the multiplicative order of i. The 9 products of the triplet (y, x, yx) are:

$$y^2, yx, y^2x; yx^i, x^2, yx^{i+1}; y^2x^i, yx^2, y^2x^{1+i}.$$

As q is odd, it is $i \neq -1$, besides $i \neq 1$. Not to get A_{51} we have only one possibility, that is $i = 2$, so $2^q \equiv 1 \pmod p$. But then we choose $y' = y^2$ instead of y so $x^{y'} = x^4$ and the 9 products of the triplet $(y', x, y'x)$ are distinct, a contradiction. It follows that G must be abelian.

Proposition 4.4. *Let G be a group of order $2^m n$, with n odd and different from 1, and suppose that $p_{51}(G) = 0$. Then, for all odd prime p, the Sylow p-subgroups are normal in G.*

Proof: Because of Theorem 4.1, G is soluble, so it possesses a Hall subgroup M of order n, which is abelian by the previous Proposition 4.3, so it sufficies to prove that M is normal in G. Let G be a minimal counterexample; using an argument similar to that of the previous proof, we can reduce to the case of $G = PM$, where P is the only minimal normal subgroup of G, it has order 2^m and n is an odd prime. Let y be a generator of M and let x be a nontrivial element of P, so that $|x| = 2$. If $r = [y, x] \in \langle x \rangle$, then $\langle x \rangle$ would be normal in G, so $\langle x \rangle = P$ and hence $P \leq Z(G)$ and G is abelian, a contradiction. Thus $m > 1$ and $r \notin \langle x \rangle$, so the triplet (y, x, yx) is associated to the matrix A_{51}, a contradiction. It follows that $M \triangleleft G$.

Proposition 4.5.

a) *If G is a dihedral group (even infinite) then $p_{51}(G) = 0$.*

b) *If G is a generalized quaternion group, then $p_{51}(G) = 0$.*

Thus the nilpotency class of G is not bounded by the condition $p_{51}(G) = 0$.

Proof: a) Let G be the infinite dihedral group:

$$G = \langle a, b \mid b^2 = 1, a^b = a^{-1} \rangle.$$

Its elements are of the form a^ib^ϵ, where $i \in Z$ and $\epsilon \in \{0,1\}$. A triplet of distinct elements of G is, for example, $\{a^ib^\epsilon, a^jb^\mu, a^kb^\nu\}$.

For $\epsilon = \mu = 1$, it is $(a^ib^\epsilon)^2 = (a^jb^\mu)^2$, and for $\epsilon = \mu = 0$ it is $a^ia^j = a^ja^i$ so the associated matrix is not A_{51}. It follows that $p_{51} = 0$.

We have already observed that the class of groups G with $p_{51} = 0$ is closed under epimorphism, so for finite dihedral groups we get $p_{51} = 0$.

b) Let $G \simeq Q_{2n+1} \simeq \langle a, b \mid a^{2^n} = b^4 = 1, a^{2^{n-1}} = b^2, a^b = a^{-1}\rangle$.

Its elements have the form a^ib^ϵ with $i \in \{0, 1, \dots, 2^n - 1\}$ and $\epsilon \in \{0,1\}$.

As before we get $p_{51} = 0$.

Remark: We observe that for the group G of order 16

$$G = \langle a, b \mid a^8 = b^2 = 1, a^b = a^3\rangle$$

it is $p_{51} \neq 0$, so $p_{51} = 0$ does not hold for all metabelian 2-groups. However the totality of known examples with $p_{51} = 0$ is metabelian. We conjecture that this is always true for nonabelian 2-groups. To support our conjecture, we have the following two partial results.

Proposition 4.6. *Let G be a 2-group with derived length at least 3. Then* $p_{49} + p_{51} \neq 0$.

Proof: Let B be a basis for G. If for every pair of elements x_i, x_j of B it were $[x_i, x_j] \in Z(G')$, then G' would be abelian; in fact every commutator is a product of conjugates of commutators $[x_i, x_j] \in Z(G') \lhd G$, so $G' = Z(G')$, a contradiction.

Therefore there exist $a, b \in B$ and $c \in G'$ such that $d = [a, b] \notin Z(G')$ and $[d, c] \neq 1_G$. The element c cannot centralize at the same time a and b, otherwise $[c, d] = 1_G$. If $[a, c] = 1_G$ then $[ad, c] = [d, c] \neq 1_G$ and $[ad, b] = [a, b]^d[d, b] = d^b \notin Z(G')$, so we can substitute a with ad. Now consider the matrix A corresponding to the triplet (a, b, c); first of all it is $a_{ij} \neq a_{ji}$ $\forall i \neq j$ because the 3 elements do not commute. Besides, B being a basis and $a, b \in B$, they are not conjugate (if it were $b = a^g$, for a suitable $g \in G$, it would be $b = a[a, g] \in aG' \subseteq a\Phi(G)$, so, in $G/\Phi(G)$ the elements $a\Phi(G)$ and $b\Phi(G)$ would not be independent). So it cannot be either $ac = cb$ or $ca = bc$. Of course, as $c \in G'$, it is not conjugate to a or b, which do not belong to G'. So $ac \neq ba$, $ca \neq ab$, $bc \neq ab$, $cb \neq ba$.

Besides it is $a^2, b^2, c^2 \in \Phi(G)$, while $ab, ac, bc, ba, ca, cb \notin \Phi(G)$ and $\{a^2, b^2, c^2\} \cap \{ab, ac, bc, ba, ca, cb\} = \emptyset$.

This means that, if $p_{51} = 0$, then $|\{a^2, b^2, c^2\}| \leq 2$, so, either $a^2 = b^2 = c^2$ and the corresponding matrix is A_{42}, or $|\{a^2, b^2, c^2\}| = 2$ and A_{49} is the unique matrix with 8 distinct elements and 2 equal squares. Consequently $p_{42} + p_{49} + p_{51} \neq 0$.

Now we show that we can choose a, b, c such that $a^2 = b^2 = c^2$ is not satisfied.

Set $H = \langle a, b\rangle$ with $a^2 = b^2$ and $S = \langle a^2\rangle$; then $S \leq Z(H)$ so $S \triangleleft H$. If H/S is not abelian, then it is dihedral and consequently $o(baS) > 2$ and so $(ba)^2 \neq b^2$. Besides $[ba, b] = [a, b] = d$, and if it were $[ba, c] = 1_G$ we would have, as above, $[bad, c] = [d, c] \neq 1_G$. Substituting a by ba (or by $ab = bad$) we get the right triplet. If H/S is abelian, then $H' \leq S$, H is nilpotent of class 2 and $H' = \langle d\rangle$.

If $|H/H'| > 4$ we get $H/H' = \langle bH'\rangle \times \langle b^{-1}aH'\rangle$ where $|bH'| > 2$ and $|\langle b^{-1}aH'\rangle| = 2$ as $d(b^{-1}a)^2 = 1$.

So $(b^{-1}a)^2 \neq b^2$ and $[b^{-1}a, b] = [a, b] = d$ and we argue as above.

Finally let $|H/H'| = 4$. As H/S is abelian and dihedral we have $|H/S| = 4$. In view of $H' \leq S$ we conclude that $H' = S$ or $\langle d\rangle = \langle a^2\rangle$.

Thus $a^2 = d^i$, i odd. If $c^2 = a^2$, then $c \in C_H(a^2) = C_H(d^i)$ and i being odd this implies that $[c, d] = 1$, contradicting our assumption. So $c^2 \neq a^2$ and the triplet (a, b, c) satisfies $|\{a^2, b^2, c^2\}| \geq 2$ yielding $p_{49} + p_{51} > 0$.

Corollary 4.7. *If the maximal number of distinct elements in the group-matrices of G is not bigger than 7, then $dl(G) \leq 2$.*

Proof: The property is inherithed by subgroups. If $|G|$ is odd, then G is abelian as $p_{51} = 0$ (see proposition 4.3). If $|G| = 2^\alpha$, then by Proposition 4.6 G is either abelian or metabelian. If $|G|$ is even, then by Proposition 4.4 the $2'$-Hall subgroup M is normal and abelian and each 2-Sylow subgroup P is at most metabelian (see Theorem C). If G is not metabelian, then P is not abelian and we can find $a, b, c \in G$ such that $a, b \in P$, $d = [a, b] \neq 1_G$ and $c \in G'$ such that $[d, c] \neq 1_G$. As P is metabelian and $G' \leq P'M$, $c \notin P$ so $c = c'c''$, $c' \in P'$, $c'' \in M$. But $[c'c'', d] = [c'', d]$ and we can suppose $c = c''$. Of course it is $c^2 \notin \{a^2, b^2\}$ and so we get either the matrix A_{49} or A_{51}, a contradiction. So G is metabelian.

References

[Fr] G.A. Freiman, On two- and three-elements subsets of groups, *Aequationes Mathematicae* **22** (1981), 140–152.

[BH] L. Brailovsky and M. Herzog, Counting squares of two-subsets in finite groups, *Ars Combinatoria* **42** (1996), 207–210.

[Hu I] B. Huppert, *Endliche Gruppen I*, Springer Verlag, Berlin (1967).

[Hu III] B. Huppert and N. Blackburn, *Finite Groups III*, Springer Verlag, Berlin (1982).