Bounds on Squares of Two–Sets

Daniel Slilaty and Jeffrey Vanderkam*

January 6, 1994

Abstract

Let G be a finite group and let $p_i(G)$ denote the proportion of $(x,y) \in G^2$ for which the set $\{x^2, xy, yx, y^2\}$ has cardinality i. We show that either $0 < p_1(G) + p_2(G) \leq 1/2$ or $p_1(G) + p_2(G) = 1$, and that either $p_4(G) = 0$ or $5/32 \leq p_4(G) < 1$. Each of the preceding inequalities are the best possible.

1 Introduction

Given two elements, x, y, not necessarily distinct, in a finite group G, we define the square of the set $\{x,y\}$ to be the set $\{x^2, xy, yx, y^2\}$.

Let

$$p_i(G) = \frac{\left|\left\{(x,y) \in G^2 : |\{x,y\}^2| = i\right\}\right|}{|G|^2}$$

for $1 \leq i \leq 4$. The values of the p_i's depend on the proportion of pairs that commute, the proportion of pairs that have equal squares, and the proportion of pairs that do both. Brailovsky and Herzog [1] have shown that

$$\begin{aligned} p_1(G) &= \frac{1}{|G|} \\ p_2(G) &= \frac{k_i - 1}{|G|} \end{aligned}$$

*The authors' work was supported by NSF Grant DMS 9100509.

$$p_3(G) = \frac{k + k_r - 2k_i}{|G|}$$
$$p_4(G) = \frac{|G| - k - k_r + k_i}{|G|},$$

where k, k_r, and k_i denote the number of conjugacy classes, real conjugacy classes (classes of elements that are conjugate to their inverses), and involution conjugacy classes (including the identity class) in G, respectively. It is clear that $p_1(G)+p_2(G) = 1$ if and only if G is an elementary abelian 2-group, and all G for which $p_4(G) = 0$ have been classified in [2]. In this paper we will find upper and lower bounds for $p_1(G)+p_2(G)$ when it is less than 1, and upper and lower bounds for $p_4(G)$ when it is greater than 0.

2 Bounds on $p_1(G) + p_2(G)$

Since $p_1(G)+p_2(G) = k_i/|G|$, to find upper and lower bounds we need only consider the possible number of involution conjugacy classes in a group. Since $k_i = 1$ whenever $|G|$ is odd, $k_i/|G|$ can be arbitrarily close to zero. We will find an upper bound for $p_1(G) + p_2(G)$ for groups G with $p_1(G) + p_2(G) < 1$, since the case where it equals 1 has already been done.

Theorem 1: *If* $p_1(G)+p_2(G) \neq 1$, *then* $0 < p_1(G)+p_2(G) \leq 1/2$, *with equality if and only if* $G \cong Z_4 \times (Z_2)^n$, *or* $G \cong D_4 \times (Z_2)^n$.

Proof: First we note that, since $G \ncong (Z_2)^n$, not all the conjugacy classes of G are involution conjugacy classes, so $k_i < k$. It is known [3] that $k/|G| = 1$ if and only if G is abelian, and that otherwise $0 < k/|G| \leq 5/8$. Rusin [5] has shown that if $1/2 < k/|G| \leq 5/8$, then $G/Z(G) \cong (Z_2)^{2n}$ for some $n \geq 1$. Since we can not have $k_i \geq 1/2$ unless $k > 1/2$, we see that if $p_1(G) + p_2(G) \geq 1/2$, then G is nilpotent, since either G or $G/Z(G)$ is abelian. As a result, $G = P_2 \times S$ where P_2 is the 2-Sylow subgroup of G and S has odd order. If S were not trivial, then

$$\frac{k_i(G)}{|G|} = \frac{k_i(P_2)}{|P_2|} \cdot \frac{k_i(S)}{|S|} \leq \frac{k_i(S)}{|S|} = \frac{1}{|S|} < \frac{1}{2},$$

so S must be trivial. Thus, G is a 2-group. We proceed by cases.

- If G is abelian, then each element forms its own conjugacy class, so to maximize $k_i/|G|$ it suffices to maximize the ratio of the number of involutions in G to $|G|$. Since $G \ncong (Z_2)^n$, the set of involutions, I, forms a proper subgroup, so $k_i/|G| = |I|/|G| \leq 1/2$. Equality in this case occurs only when $G \cong Z_4 \times (Z_2)^n$, since no other abelian group has an involution subgroup half its size.

- If G is not abelian, then, as shown by Miller in [4], $|I| \leq \frac{3}{4}|G|$. Thus,

$$\begin{aligned} k_i &\leq |I \cap Z(G)| + \frac{1}{2}|I - Z(G)| \\ &\leq |Z(G)| + \frac{1}{2}(|I| - |Z(G)|) \\ &= \frac{1}{2}|Z(G)| + \frac{1}{2}|I| \\ &\leq \frac{1}{8}|G| + \frac{3}{8}|G| \\ &= \frac{1}{2}|G|. \end{aligned}$$

  As for the equality condition, Miller [4] has shown that $I = \frac{3}{4}|G|$ implies that $G \cong D_4 \times (Z_2)^n$. Since $p_1(G) + p_2(G) = 1/2$ in this case, the proof is complete.

3 Bounds on $p_4(G)$

We note that $|\{x^2, xy, yx, y^2\}| = 4$ if and only if x and y neither commute nor have equal squares. Freiman [2] has shown that $p_4(G) = 0$ if and only if G is abelian or $G \cong Q \times Z_2^n$, where Q is the quaternion group of order eight. In this section we will demonstrate both upper and lower bounds for $p_4(G)$ when it is nonzero, and we will show the sharpness of each.

Theorem 2: *The least upper bound for $p_4(G)$ is 1.*

Proof: First note that $p_4(G) < 1$ because $p_1(G) > 0$ for all G. We construct a sequence (G_n) of groups for which $p_4(G_n) \to 1$. Let $G_n = (D_4)^n$. Since $k(D_4) = 5$ and $k(G \times H) = k(G)k(H)$, there are

exactly 5^n conjugacy classes in G_n. Since $p_4(G) > (|G| - 2k)/|G|$ for any group G, this gives

$$p_4(G_n) > 1 - 2 \cdot (\frac{5}{8})^n,$$

and the result follows. Clearly, D_4 can be replaced here by any nonabelian group G.

Theorem 3: *If $p_4(G) > 0$, then $p_4(G) \geq 5/32$.*

We begin by proving four lemmas that deal with the structure of potential counterexamples.

Lemma 1: *If $n \geq 1$ and Q is the quaternion group of order eight, then $p_4(Z_{2n+1} \times Q) \geq 1/4$.*

Proof: Let (x, y) be a pair of elements in $Z_{2n+1} \times Q$. The pair does not commute if and only if its projections in Q do not commute, and this happens with probability $3/8$. Since all non-commuting elements of Q have the same square, a non-commuting pair in $Z_{2n+1} \times Q$ has unequal squares if and only if its projections in Z_{2n+1} are distinct. This happens in exactly $2n/(2n+1)$ of the pairs. It follows that

$$\begin{aligned} p_4(Z_{2n+1} \times Q) &= \left(\frac{3}{8}\right)\left(\frac{2n}{2n+1}\right) \\ &= \frac{3n}{8n+4}, \end{aligned}$$

which is an increasing function of n and takes the value $1/4$ at $n = 1$.

Lemma 2: *If N is a normal subgroup of G, then $p_4(G/N) \leq p_4(G)$.*

Proof: If two elements in G have the same square, so do their images in G/N. If two elements of G commute, so do their images in G/N. Thus, $p_1(G/N)+p_2(G/N)+p_3(G/N) \geq p_1(G)+p_2(G)+p_3(G)$, and the result follows.

Lemma 3: *If $p_4(G) \leq 5/32$, then $k(G) > \frac{27}{64}|G|$.*

Proof: We recall that $p_4(G) = (|G| - k - k_r + k_i)/|G| > (|G| - 2k)/|G|$. Thus, if $k \leq \frac{27}{64}|G|$, then $p_4(G) > 5/32$.

Rusin [5] has shown that the only groups with $k(G) > \frac{27}{64}|G|$ are those G such that $G/Z(G)$ is isomorphic to $(Z_2)^n, D_4$, or S_3. Now $p_4(D_4) = 1/4$ and $p_4(S_3) = 1/3$, so by Lemma 2, $G/Z(G)$ cannot be either D_4 or S_3 if $p_4(G) \leq 5/32$. Thus if $0 < p_4(G) \leq 5/32$, we know that $G/Z(G)$ is an elementary abelian 2-group.

Lemma 4: *If G is a group of minimal order such that $0 < p_4(G) \leq 5/32$, then G is a 2-group.*

Proof: As we have seen, $G/Z(G)$ is an elementary abelian 2-group, so G is nilpotent. As a result, we may write $G \cong P_1 \times \cdots \times P_m$, where the P_i's are the unique p_i-Sylow subgroups of G. Since $G/Z(G)$ is a (non- trivial) 2-group, we may assign P_1 to be the 2-Sylow subgroup of G. We will show that there are no other Sylow subgroups. Suppose instead that $P_2, \ldots, P_m$ are non-trivial. Every Sylow subgroup is a quotient group of G, so by Lemma 2 they each have a p_4 value that is no greater than that of G. By the minimality of G, this means that $p_4(P_i) = 0$ for all i. By [2], this can only happen if P_i is abelian for every $i > 1$, and either P_1 is abelian or $P_1 \cong Q \times (Z_2)^r$ for some integer r. If P_1 is abelian, then G is the direct product of abelian groups, so G is abelian, an impossibility. Thus $P_1 \cong Q \times (Z_2)^r$. But P_2 is the direct product of cyclic groups of odd order, so the group $Q \times Z_{2n+1}$ is a quotient group of G for some positive n. But by Lemma 1, this has a p_4 value that is at least $1/4$, so by Lemma 2, $p_4(G) \geq 1/4$, contradicting $p_4(G) \leq 5/32$.

Proof of Theorem: Let G be a group of minimal order for which $0 < p_4(G) < 5/32$. From the previous lemmas, we know that G must be a 2-group with more than $\frac{27}{64}|G|$ conjugacy classes. Rusin [5] has shown that G must be one of the following two types:

1. $G' \cong (Z_2)^2$, $G' \subseteq Z(G)$, $G/Z(G) \cong (Z_2)^3$ or $(Z_2)^4$,
2. $G' \cong Z_2$, $G' \subseteq Z(G)$, $G/Z(G) \cong (Z_2)^{2n}$, where $n \geq 1$.

Case 1: The group G is of type 1 in the above list. In such groups, $k = \frac{7}{16}|G|$, so $k_r \leq \frac{7}{16}|G|$. Now if $Z(G)$ is not elementary abelian, then at least half of the elements in $Z(G)$ have order at least four. Hence at least $|Z(G)|/2$ conjugacy classes are not real, so $k_r \leq k - \frac{1}{2}|Z(G)| \leq k - \frac{1}{32}|G| = \frac{13}{32}|G|$. But then $k + k_r \leq \frac{27}{32}|G|$, and since there are at least four involution conjugacy classes (those

in G',), $k + k_r - k_i < \frac{27}{32}|G|$, so $p_4(G) > 5/32$. Thus if $p_4(G) \leq 5/32$, $Z(G) \cong (Z_2)^n$. But then, if $n > 2$, we may write $Z(G) \cong G' \times H$, where $H \cong (Z_2)^{n-2}$. We note that H is a normal subgroup of G, and that $(G/H)' = Z(G/H) \cong Z_2 \times Z_2$. By [5], the number of conjugacy classes of G/H is still $7/16$ the size of the group (the proportion of conjugacy classes cannot decrease when taking quotients, and there is no higher fraction of conjugacy classes possible in a non-abelian group if the center is $Z_2 \times Z_2$. But then $p_4(G/H) > 0$, since $k(G/H) = \frac{7}{16}|G/H|$, and $p_4(G/H) \leq p_4(G)$, contradicting the minimality of G. Thus $n = 2$, so $Z(G) = G' = (Z_2)^2$. But this means that $|G| \leq 64$, while $k_i \geq 4$, so $k_i \geq \frac{1}{16}|G|$. Thus

$$\begin{aligned} p_4(G) &= \frac{|G| - k - k_r + k_i}{|G|} \\ &\geq \frac{|G| - 2k + k_i}{|G|} \\ &\geq \frac{|G| - \frac{7}{8}|G| + \frac{1}{16}|G|}{|G|} \\ &= \frac{3}{16}, \end{aligned}$$

contradicting $p_4(G) < 5/32$, so this case is complete.

Case 2: The group G is of type 2 in the above list, and $n = 1$. In this case, $|G| = 2^{m+3}$, where $|Z(G)| = 2^{m+1}$, and $k = 5|G|/8 = 5(2^m)$. We write $G' = \{e, z\}$, where $z^2 = e$, and we denote by I_Z the involution subgroup of the center (note that $|I_Z|$ divides 2^{m+1}). We again denote the number of cosets of $Z(G)$ that contain an involution by A, and note that, as before, an element y not in $Z(G)$ that is not an involution is in a real conjugacy class if and only if $y^2 = z$. Let x be an involution not in the center. Then an element of the form xt, with $t \in Z(G)$, is an involution if and only if $e = (xt)^2 = x^2t^2 = t^2$, that is, t is an involution. Similarly, if $w^2 = z$, then an element of the form wt, with $t \in Z(G)$, has square z if and only if $z = (wt)^2 = w^2t^2 = zt^2$, that is, t is an involution. Thus, if a coset contains an involution, it contains exactly $|I_Z|$ involutions, and if it contains an element whose square is z, then it contains exactly $|I_Z|$ such elements. We consider two cases, based on whether z is the square of an element in $Z(G)$.

1. There exists $t \in Z(G)$ such that $t^2 = z$. Then $|I_Z| \leq 2^m$, since

$|I_Z| \neq |Z(G)|$. We prove that a coset contains involutions if and only if it contains elements whose square is z. Suppose that x is an involution. Then $xt \in xZ(G)$, and $(xt)^2 = x^2t^2 = z$. Now suppose that y is an element whose square is z. Then $yt \in yZ(G)$ and $(yt)^2 = y^2t^2 = z^2 = e$. Thus the total number of involution conjugacy classes is exactly $k_i = \frac{1}{2}(A-1)|I_Z| + |I_Z| = \frac{1}{2}(A+1)|I_Z|$, and the total number of real conjugacy classes which are not involution conjugacy classes is $k_r - k_i = \frac{1}{2}(A-1)|I_Z|$. Then

$$\begin{aligned} p_4(G) &= \frac{|G| - k - (k_r - k_i)}{|G|} \\ &= \frac{3 \cdot 2^m - \frac{1}{2}(A-1)|I_Z|}{2^{m+3}} \\ &\geq \frac{3 \cdot 2^m - \frac{1}{2}(3 \cdot 2^m)}{2^{m+3}} \\ &= \frac{3}{16}. \end{aligned}$$

2. There is no element in $Z(G)$ whose square is z. We prove that no coset of $Z(G)$ contains both an involution and an element whose square is z. Otherwise there would be an involution x such that $(xt)^2 = z$ for some $t \in Z(G)$, in which case $z = (xt)^2 = x^2t^2 = t^2$, a contradiction. We denote by B the number of cosets of $Z(G)$ that contain an element whose square is z, and note that $B + A \leq 4$, and since $A \geq 1$, $B \leq 3$. The number of real conjugacy classes that are not involution conjugacy classes is then $k_r - k_i = B|I_Z|/2$. Now if $|I_Z| \leq 2^m$, this gives the same series of inequalities as the last case (with B replacing $A-1$), so we need only consider $|I_Z| = |Z(G)|$, that is, the case in which $Z(G) \cong (Z_2)^{m+1}$. Then

$$\begin{aligned} p_4(G) &= \frac{2^{m+3} - 2^{m+2} - 2^m - \frac{1}{2}B(2^{m+1})}{2^{m+3}} \\ &= \frac{3 - B}{8}. \end{aligned}$$

If $B = 3$, then $p_4(G) = 0$, and if $B = 1$, then $p_4(G) = 1/4 > 5/32$, so we need only show that B cannot equal 2. Suppose

instead that it does. Then let x and y be two elements whose squares are z but which are in different cosets of the center. Now x commutes with all of $Z(G)$ and all of $xZ(G)$, so it cannot commute with y, since then it would commute with over half of the elements of the group. As a result, $[x,y] = xyx^{-1}y^{-1} = z$. But $x^2 = y^2 = z$, $x^{-1} = xz$ and $y^{-1} = yz$, so $z = xy(xz)(yz) = xyxyz^2 = (xy)(xy)$. This means that the fourth coset of the center, $xyZ(G)$, also contains an element whose square is z, namely xy, contradicting $B = 2$. This completes the proof of this case.

Case 3: The group G is of type 2 in the above list with $n \geq 2$. Note that every conjugacy class in such a group has size either 1 or 2. We show that $Z(G)$ must be cyclic. Assume instead that $Z(G) \cong Z_{2^a} \times H$, where $G' \not\subseteq Z_{2^a}$. Then $p_4(G/Z_{2^a}) > 0$, since G/Z_{2^a} is not isomorphic to $Q \times (Z_2)^n$ (since the index of its center is larger than four), and $p_4(G/Z_{2^a}) \leq p_4(G)$, contradicting the minimality of G. Thus, in a minimal G with $|G/Z(G)| \geq 16$, $Z(G)$ is cyclic. We write $Z(G) = \langle z \rangle$, with $|z| = 2^{m+1} = |Z(G)|$. The order of G is thus 2^{2n+m+1}, the number of conjugacy classes in G is $2^{2n+m} + 2^m$, and G' consists of e and z^{2^m}, the only two involutions in $Z(G)$. We consider the 2^{2n} cosets of $Z(G)$, and we show that the number of involutions in a given coset is equal to either two or zero. Suppose that x is an involution. If xz^i is an involution, then $e = (xz^i)(xz^i) = x^2z^{2i} = z^{2i}$, so either $i = 0$ or $i = 2^m$. Either of these values for i clearly yields an involution, so there are exactly two involutions in the coset $xZ(G)$. We note also that since $G/Z(G)$ is abelian, cosets of $Z(G)$ are fixed under conjugation, so the two involutions in the coset $xZ(G)$ must be conjugate, since they are the only elements in the coset to have order 2. If we denote the number of cosets of the center containing an involution by A, this means that $k_i = (A-1) + 2 = A + 1$, since there are two involution conjugacy classes in the center. Now we consider the number of real conjugacy classes. Since all conjugacy classes outside the center of G have size two, the only possible real conjugacy classes that are not involution conjugacy classes are those containing only an element and its inverse. Now suppose y is in a real conjugacy class and is not an involution. There must be some element $w \in G$ such that $w^{-1}ywy^{-1} = z^{2^m}$, since the derived group contains

only two elements. But then $w^{-1}yw = yz^{2^m}$, and $y^{-1} = yz^{2^m}$, so the order of y is four. Since $G/Z(G)$ is an elementary abelian 2-group, the square of each element is in the center, so an element has order four if and only if its square is z^{2^m}, the only element in the center with order two. Thus, the number of real conjugacy classes that are not involution conjugacy classes must equal half the number of elements not in the center with order four. We now divide the proof into two cases, depending on the value of m.

1. First we consider the case $m \geq 1$. We will show that if an element has order four, then its coset of the center also contains an involution. Suppose that $|y| = 4$. Then $y^2 = z^{2^m} = (z^{2^{m-1}})^2$, so $yz^{-(2^{m-1})}$ is an involution in the coset containing y. But if x is an involution, then $(xz^i)^2 = z^{2^m}$ if and only if $i = 2^{m-1}$ or $i = 3 \cdot 2^{m-1}$. Thus there are exactly two elements with order four in each coset containing an involution, so the total number of elements of order four that are not contained in the center equals $2(A-1)$, and $k_r = k_i + (A-1) = 2A$. Thus

$$\begin{aligned}
p_4(G) &= \frac{|G| - k - k_r + k_i}{|G|} \\
&= \frac{2^{2n+m+1} - 2^{2n+m} - 2^m - 2A + A + 1}{2^{2n+m+1}} \\
&= \frac{2^{2n+m} - 2^m - A + 1}{2^{2n+m+1}} \\
&\geq \frac{2^m(2^{2n}-1) - (2^{2n}-1)}{2^{2n+m+1}} \\
&= \frac{1}{2}\left(\frac{2^m - 1}{2^m}\right)\left(\frac{2^{2n}-1}{2^{2n}}\right) \\
&\geq \left(\frac{1}{2}\right)\left(\frac{1}{2}\right)\left(\frac{15}{16}\right) \\
&= \frac{15}{64},
\end{aligned}$$

contradicting $p_4(G) < 5/32$.

2. Now we consider the case $m = 0$. Here $Z(G) = G' \cong Z_2$, $|G| = 2^{2n+1}$, and $k = 2^{2n} + 1$. Since conjugation fixes cosets of the center, and each element shares a coset of the center

with its inverse, all conjugacy classes are real, so $k_r = 2^{2n} + 1$. Since every element's square is either e or z, the number of pairs with equal squares is (number of elements with square $e)^2$ + (number of elements with square $z)^2$. The total number of involutions is still $2A$, so this is $(2A)^2 + (2^{2n+1} - 2A)^2$. By [1], the number of pairs with equal squares is $k_r|G| = 2^{4n+1} + 2^{2n+1}$, so

$$\begin{aligned} 2^{4n+1} + 2^{2n+1} &= 4A^2 + 2^{4n+2} - 2^{2n+3}A + 4A^2 \\ 0 &= A^2 - 2^{2n}A + 2^{4n-2} - 2^{2n-2} \\ A &= 2^{2n-1} \pm 2^{n-1}. \end{aligned}$$

Thus, $k_i \geq 2^{2n-1} - 2^{n-1} + 1$, so

$$\begin{aligned} p_4(G) &\geq \frac{2^{2n+1} - 2(2^{2n} + 1) + 2^{2n-1} - 2^{n-1} + 1}{2^{2n+1}} \\ &= \frac{2^{2n-1} - 2^{n-1} - 1}{2^{2n+1}} \\ &\geq \frac{5}{32}, \end{aligned}$$

with equality only if $n = 2$. Using the computer algebra system CAYLEY, we found a group of order 32 with $p_4(G) = \frac{5}{32}$ that had these properties, namely the central product of Q and D_4. Since we have shown the existence and sharpness of the lower bound, the proof is complete.

References

[1] Brailovsky, L. and M. Herzog. *Lemma on squares of 2-element sets.* Unpublished note.

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

[3] Gustafson, W. H. *What is the probability that two group elements commute?* The American Mathematical Monthly **80** (1973), pp. 1031-1034.

[4] Miller, G. A. *Groups Containing the Largest Possible Number of Operators of Order Two.* The American Mathematical Monthly **11** (1905), pp. 149-150.

[5] Rusin, David J. *What is the probability that two elements of a finite group commute?* Pacific Journal of Mathematics **82** (1979), pp. 237 - 247.