5-1993

Bounds on Squares of Two-Sets

Dan Slilaty
Rose-Hulman Institute of Technology

Jeff Vanderkam
Rose-Hulman Institute of Technology

BOUNDS ON SQUARES OF TWO-SETS

Dan Slilaty and Jeff Vanderkam

MS TR 93-04

May 1993

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 **Phone: (812) 877-8391**

Bounds on Squares of Two–Sets

Daniel Slilaty and Jeff Vanderkam*

May 26, 1993

Abstract

Let G be a finite group and let $p_i(G)$ denote the proportion of $(x,y)\epsilon G^2$ for which the set $\{x^2, xy, yx, y^2\}$ has cardinality i. In this paper we show that:

$p_1(G) + p_2(G) \neq 1$ implies $0 < p_1(G) + p_2(G) \leq 1/2$,

$p_4(G) \neq 0$ implies $5/32 \leq p_4(G) < 1$.

1 Terminology, notation and facts

In this paper G always denotes a finite group and

- $k = k(G)$ is the number of conjugacy classes in G,
- $k_r = k_r(G)$ is the number of real conjugacy classes in G,
- $k_i = k_i(G)$ is the number of involution conjugacy classes in G.

Fact 1 $k_i \leq k_r \leq k$.

*Both authors supported by NSF Grant NSF–DMS 9100509

This follows because involution conjugacy classes are real conjugacy classes and real conjugacy classes are conjugacy classes. Notice also that $k_i = k$ if and only if $x^2 = 1$ for each $x \epsilon G$; i.e. G is an elementary abelian two–group.

For $(x, y) \epsilon G^2$ we refer to $\{x, y\}$ as a two-set even though $|\{x, y\}|$ may be one. Indeed there are $|G|^2 - |G|$ two-sets of cardinality two and there are $|G|$ two-sets of cardinality one.

We are concerned with

$$|\{x, y\}^2| = |\{x^2, xy, yx, y^2\}|$$

which depends on whether x and y commute or have the same squares.

Fact 2 *[4] The number of pairs in G that commute is $k \cdot |G|$.*

Fact 3 *[1] The number of pairs in G with equal squares is $k_r \cdot |G|$.*

Fact 4 *[1] The number of pairs in G that commute and have equal squares is $k_i \cdot |G|$.*

Let

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

for $1 \leq i \leq 4$.

Fact 5

$$p_1(G) = \frac{1}{|G|}.$$

This follows because $x^2 = yx$ if, and only if, $x = y$.

Fact 6

$$p_2(G) = \frac{k_i - 1}{|G|}.$$

This follows because $|\{x,y\}^2| = 2$ if, and only if $x^2 = y^2$, $xy = yx$, and $x \neq y$.

Fact 7

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

Notice that $p_3(G) = 0$ if, and only if, $G \cong Z_2^n$.

Fact 8

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

2 Bounds on $p_1(G) + p_2(G) = k_i/|G|$

Since $k_i = 1$ if, and only if, $|G|$ is odd, $p_1(G) + p_2(G)$ can be arbitrarily close to zero. And, if G is an elementary abelian 2–group, then $p_1(G) + p_2(G) = 1$. The remainder of this section will be devoted to the proof of the following theorem:

Theorem 1 *If* $p_1(G) + p_2(G) \neq 1$, *then* $0 < p_1(G) + p_2(G) \leq 1/2$.

Before beginning the proof of this theorem we record three more facts and prove a lemma.

Fact 9 $p_1(Z_4) + p_2(Z_4) = p_1(D_4) + p_2(D_4) = 1/2$.

Fact 10 *If* $G \ncong Z_2^n$ *then* $\dfrac{k_i}{|G|} < \dfrac{k}{|G|}$

Notice that $k/|G|$ may be interpreted as the probability that two random elements commute. It is well known [4] that if $k/|G| \neq 1$, then $0 < k/|G| \leq 5/8$.

Fact 11 *[4] If* $1/2 < k/|G| \leq 5/8$, *then*

i) each conjugacy class of G *contains either one or two elements,*

ii) $G' = Z_2$,

iii) $G' \subseteq Z(G)$,

iv) $G/Z(G) \cong Z_2^{2n}$ $(n \geq 1)$.

Lemma 1 *If* $p_1(G) + p_2(G) \geq 1/2$, *then* G *is a 2-group.*

PROOF: It follows from Facts 10 and 11 that G is nilpotent. Let $G = H \oplus S$ where H is the 2–Sylow subgroup of G and S has odd order. If S is not trivial, then

$$\begin{aligned} \frac{k_i(G)}{|G|} &= \frac{k_i(H)}{|H|} \cdot \frac{k_i(S)}{|S|} \\ &\leq \frac{k_i(S)}{|S|} \\ &= \frac{1}{|S|} \\ &< \frac{1}{2}, \end{aligned}$$

a contradiction.

PROOF OF THEOREM: In view of the previous lemma it is only necessary to analyze 2–groups. We proceed by cases.

If G is abelian, then each element is a conjugacy class. Thus, 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 all involutions of G, I, forms a proper subgroup. Therefore, $k_i|G| = |I|/|G| \leq 1/2$.

If G is non–abelian, then $|I| \leq 3 \cdot |G|/4$ (see [2]). Thus,

$$\begin{aligned} \frac{k_i}{|G|} &\leq \frac{|Z(G)| + \frac{|I|-|Z(G)|}{2}}{|G|} \\ &\leq \frac{|Z(G)| + \frac{3\cdot|G|/4-|Z(G)|}{2}}{|G|} \\ &= \frac{|Z(G)|/2 + 3 \cdot |G|/8}{|G|} \end{aligned}$$

$$\leq \frac{|G|/8 + 3 \cdot |G|/8}{|G|}$$
$$= \frac{1}{2}.$$

Corollary 1 *If G is non-abelian and $p_1(G) + p_2(G) = 1/2$, then $k/|G| = 5/8$.*

PROOF: It is evident from the proof of the theorem that $G/Z(G) = Z_2 \oplus Z_2$. This implies that $k/|G| = 5/8$ (see [4]).

3 Bounds on $p_4(G)$

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

PROOF: First note that $p_4(G) \neq 1$ because $|\{x, x\}^2| = 1$ for each $x \epsilon G$. We construct a sequence $\{G_n\}$ of groups for which $p_4(G_n) \to 1$. Let $G_n = D_4^n$. It follows that

$$1 - 2 \cdot (5/8)^n < p_4(G_n)$$

because $k(D_4) = 5$, $k(G \oplus H) = k(G) \cdot k(H)$, and $(|G| - 2k)/|G| < p_4(G)$. Since $1 - 2 \cdot (5/8)^n \to 1$ the result follows. Notice that D_4 can be replaced by any group with $p_4(G) \neq 0$.

Frieman [3] has shown that $p_4(G) = 0$ if, and only if, G is abelian or $G \cong Q \oplus Z_2^n$, where Q is the quaternion group. This section will be devoted to the proof of the following theorem.

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

This inequality is in fact sharp as the group of order 32 with generators,

$$a_1, a_2, a_3, a_4,$$

and relations,

$$a_1{}^2 = a_4{}^2 = 1,$$

$$a_2{}^2 = a_3{}^2,$$

$$[a_2, a_1] = [a_3, a_2] = [a_4, a_1],$$

$$[a_i, a_j] = 1 \text{ for } (i,j) \neq (2,1),(1,2),(3,2),(2,3),(4,1),(1,4),$$

has $p_4 = 5/32$.

We begin by proving four lemmas.

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

PROOF: Let $x, y \epsilon (Z_{2n+1} \oplus Q)^2$. Clearly, x and y do not commute if, and only if, their 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 $Z_{2n+1} \oplus Q$ has unequal squares if, and only if, their projections in Z_{2n+1} are distinct. This happens with probability $2n/(2n+1)$. It follows that

$$\begin{aligned} p_4(Z_{2n+1} \oplus Q) &= \frac{3}{8} - \frac{2n}{2n+1} \\ &= \frac{3n}{8n+4} \end{aligned}$$

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

Lemma 3 *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 in G/N 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.

Now, using Fact 8, it is possible to place restrictions on which groups can have $p_4(G) \leq 5/32$.

Lemma 4 *If $p_4(G) \leq 5/32$, then the number of conjugacy classes in G is greater than $27|G|/64$.*

PROOF: Recall that $p_4(G) > (|G| - 2k)/|G|$. Thus, if $k \leq 27|G|/64$, then $p_4(G) > 5/32$.

It is known [4] that the only groups with $k > 27|G|/64$ 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 3, G/Z cannot equal 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 5 *If G is the 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 $G = P_1 \oplus \cdots \oplus P_m$, 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. Then every Sylow subgroup is a quotient group of G, so by Lemma 3 they each have a p_4 value that is no greater than that of G. But since G was minimal, this means that $p_4(P_i) = 0$ for all i. This can only happen [3] if P_i is abelian for every $i > 1$, and either P_1 is abelian or $P_1 \cong Q \oplus (Z_2)^r$ for some integer r. If P_1 is abelian, then G is the direct product of abelians, so G is abelian, an impossibility. Thus $P_1 \cong Q \oplus (Z_2)^r$. But P_2 is the direct product of cyclic groups of odd order, so the group $Q \oplus Z_{2n+1}$ is a quotient group of G for some positive n. But by Lemma 2, this has a p_4 value that is at least $1/4$, so by Lemma 3, $p_4(G) \geq 1/4$, contradicting $p_4(G) \leq 5/32$.

PROOF OF THEOREM: From the preceeding lemma, we see that we need only examine the 2–groups to show that $p_4(G) \geq 5/32$ or $p_4(G) = 0$ for all G. We break the 2–groups with more than $27|G|/64$ conjugacy classes into 2 cases, based on the classification of groups given in [4].

Case 1: The minimal group G such that $0 < p_4(G) \leq 5/32$ is of the type $G' \cong Z_2 \oplus Z_2$, $G' \subseteq Z(G)$, $G/Z(G) \cong (Z_2)^3$ or $(Z_2)^4$. In such groups, $k = 7|G|/16$, so $k_r \leq 7|G|/16$. Now if

$Z(G) \ncong (Z_2)^n$, then at least half of the elements in $Z(G)$ have order at least four. This means that at least $|Z(G)|/2$ conjugacy classes are not real, so $k_r \leq k - |Z(G)|/2 \leq k - |G|/32 = 13|G|/32$. But then $k + k_r \leq 27|G|/32$, and since there is are at least four involution conjugacy classes (those in G',), $k + k_r - k_i < 27|G|/32$, 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 $Z(G) \cong G' \oplus (Z_2)^{n-2} = G' \oplus H$. We note that H is a normal subgroup of G, and that $(G/H)' = Z(G/H) \cong Z_2 \oplus Z_2$. By [4], the number of conjugacy classes of G/H is still $7/16$ the size of the group (the relative number 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 the Klein 4-group). But then $p_4(G/H) > 0$, since $k = 7|G/H|/16 < 1/2$, and $p_4(G/H) \leq p_4(G)$, contradicting the minimality of G. Thus $n = 2$, so $Z(G) = G' = Z_2 \oplus Z_2$. But this means that $|G| \leq 64$, while $k_i \geq 4$, so $k_i \geq |G|/16$. Thus $p_4(G) = (|G| - k - k_r + k_i)/|G| \geq (|G| - 2k + k_i)/|G| \geq (|G| - 7|G|/8 + |G|/16)/|G| = 3/16 > 5/32$, so this case is complete.

Case 2: The minimal group G such that $0 < p_4(G) \leq 5/32$ is of the type $G' \cong Z_2$, $G' \subseteq Z(G)$, $G/Z(G) \cong (Z_2)^{2n}$, where $n \geq 1$. Note that every conjugacy class in such a group has size either 1 or 2. We consider two cases based on the value of n.

- First we consider the case $n \geq 2$, and show that if G is minimal such that $p_4(G) \leq 5/32$, $Z(G)$ must be cyclic. Assume instead that $Z(G) \cong Z_{2^a} \oplus H$, where $G' \not\subseteq Z_{2^a}$. Then $p_4(G/Z_{2^a}) > 0$, since it is not equal to $Q \otimes (Z_2)^n$ (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 the 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 $G' = \{e, z^{2^m}\}$, 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 $e = (xz^i)(xz^i) = x^2 z^{2i} = z^{2i}$, 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 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 order two, the only possible real conjugacy classes which 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 $w^{-1}yw = yz^{2^m}$, so $y^{-1} = yz^{2^m}$, so $y^2 = z^{2^m}$, which implies that the order of y is four. Since $G/Z(G)$ is elementary abelian, the squares of every element are in the center, so an element has order four if, and only if, its square is z^{2m}, the only element in the center with order two. Thus, the number of real conjugacy classes which 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.

First we consider the case $m \geq 1$, and show that if an element has order four, it is contained in a coset which 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 $i = 3(2^{m-1})$. Thus there are only two elements with order four in cosets containing involutions, so the total number of elements of order four which are not contained in the center is equal to $2(A-1)$, and $k_r = k_i + (A-1) = 2A$. But then

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

$$
\begin{aligned}
&= \frac{2^{2n+m+1} - 2^{2n+m} - 2^m - 2A + A + 1}{2^{2n+m+1}} \\
&= \frac{2^{2n+m} - 2^m - A + 1}{2^{2n+m+1}} \\
&\geq \frac{2^m(2^{2n} - 1) - (2^{2n} - 1)}{2^{2n+m+1}} \\
&= \frac{1}{2}(\frac{2^m - 1}{2^m})(\frac{2^{2n} - 1}{2^{2n}}) \\
&\geq (\frac{1}{2})(\frac{1}{2})(\frac{15}{16}) \\
&= \frac{15}{64} \\
&> \frac{5}{32}.
\end{aligned}
$$

Now we consider the case $m = 0$, in which $Z(G) = G' \cong Z_2$, $|G| = 2^{2n+1}$, and $k = 2^{2n} + 1$. Every element in such a group has order four or less (since the center has order two), so every element is contained in a real conjugacy class, and $k_r = k = 2^{2n} + 1$. Since every element squares to either e or z, we may easily count the number of pairs with equal squares as (number of elements with square e)^2 + (number of elements with square z)^2. The total number of involutions is still $2A$, so we may write this as $(2A)^2 + (2^{2n+1} - 2A)^2$. By [1], the number of pairs with equal squares is equal to $k_r|G| = 2^{4n+1} + 2^{2n+1}$, we may write

$$
\begin{aligned}
2^{4n+1} + 2^{2n+1} &= 4A^2 + 2^{4n+2} - 2^{2n+3}A + 4A^2 \\
&= 8(A^2 - 2^{2n}A + 2^{4n-1}) \\
2^{4n-2} + 2^{2n-2} &= A^2 - 2^{2n}A + 2^{4n-1} \\
0 &= A^2 - 2^{2n}A + 2^{4n-2} - 2^{2n-2} \\
A &= \frac{2^{2n} \pm \sqrt{2^{4n} - 2^{4n} + 2^{2n}}}{2} \\
&= 2^{2n-1} \pm 2^{n-1}.
\end{aligned}
$$

Thus $k_i \geq 2^{2n-1} - 2^{n-1} + 1$, so $p_4(G) \geq (2^{2n+1} - 2(2^{2n} + 1) + 2^{2n-1} - 2^{n-1} + 1)/2^{2n+1} = (2^{2n-1} - 2^{n-1} - 1)/2^{2n+1} \geq 5/32$, with equality only if $n = 2$.

- Now we consider $n = 1$. 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 N_i the number of involutions in $Z(G)$ (note that N_i divides 2^{m+1}, because the involutions in the center form a subgroup of the center). We again denote the number of cosets of $Z(G)$ which contain an involution by A, and note that, as before, an element y which is not an involution is in a real conjugacy class if, and only if, $y^{-1} = yz$, or equivalently, $y^2 = z$. We consider the four cosets of $Z(G)$, and again denote by A the number which contain involutions. First we show that if a coset contains an involution, then it contains exactly N_i involutions, and if it contains an element whose square is z, then it contains exactly N_i such elements. Assume that $x^2 = e$. Then the elements of the coset $xZ(G)$ are all of the form xt, where $t \in Z(G)$. But $e = (xt)^2 = x^2t^2 = t^2$ if, and only if, t is an involution. Similarly, we assume that $y^2 = z$ and note that $z = (yt)^2 = y^2t^2 = zt^2$ if, and only if, t is an involution. Thus both values are equal to N_i. Now we consider two cases, depending on whether z is the square of an element in $Z(G)$.

  1. There exists $w \in Z(G)$ such that $w^2 = z$. This implies that $N_i \leq 2^m$, since $N_i \neq |Z(G)|$. We prove that a coset contains involutions if, and only if, it contains elements which square to z. Suppose that x is an involution. Then $xw \in xZ(G)$, and $(xw)^2 = x^2w^2 = z$. Now suppose that y is an element which squares to z. Then $yw \in yZ(G)$ and $(yw)^2 = y^2w^2 = z^2 = e$. Thus the total number of involution conjugacy classes is exactly $k_i = (A-1)N_i/2 + N_i = (A+1)N_i/2$, and the total number of real conjugacy classes which are not involution conjugacy classes is $k_r - k_i = (A-1)N_i/2$. We may then write

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

$$= \frac{3}{16}$$
$$> \frac{5}{32}.$$

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 which squares to z. Suppose instead that there is an involution x such that $(xw)^2 = z$ for some $w \in Z(G)$. Then $z = (xw)^2 = x^2w^2 = w^2$, a contradiction. We denote by B the number of cosets of $Z(G)$ which contain an element which squares to z, and note that $B + A \leq 4$, and since $A \geq 1$, $B \leq 3$. The number of real conjugacy classes which are not involution conjugacy classes is then $k_r - k_i = BN_i/2$. Now if $N_i \leq 2^m$, this gives the same series of inequalities as the last case (with B substituting for $A - 1$), so we need only consider $N_i = |Z(G)|$, that is, the case in which $Z(G) \cong (Z_2)^{m+1}$. But then

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

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 two of the four cosets contain elements which square to z. We call these elements x and y. Now x commutes with all of $Z(G)$ and all of $xZ(G)$, so it cannot commute with any element in $yZ(G)$, since then it would commute with over half of the elements of the group. Thus $[x, y] = xyx^{-1}y^{-1} = z$. But since $x^2 = y^2 = z$, $x^{-1} = xz$ and $y^{-1} = yz$. Thus we may write $z = xy(xz)(yz) = xyxyz^2 = (xy)(xy)$. This means that the fourth coset of the center, $xyZ(G)$, also contains an element whose square is z, meaning that in fact $B = 3$. This completes the proof of this case, and with it the proof of Theorem 3.

References

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

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

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

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