5-1991

An Upper Bound for 3-Rewriteability in Finite Groups

Jordan Ellenberg
Harvard University

AN UPPER BOUND FOR 3-REWRITEABILITY IN FINITE GROUPS

Jordan Ellenberg

MS TR 91-02

May 1991

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

FAX(812) 877-3198

Phone: (812) 877-8391

An Upper Bound For 3-Rewriteability in Finite Groups

Jordan Ellenberg*
Harvard University

1. Introduction

An ordered triple of group elements (x,y,z) is defined to be *rewriteable* if the product xyz is equal to one of the products xzy, yxz, yzx, zxy, or zyx. If every ordered triple of elements in a group G is rewriteable, then G is called a 3-rewriteable group. Such groups have been classified by Curzio, Longobardi, and Maj[**1**]; they are precisely those in which every conjugacy class has order 1 or 2. Equivalently, the 3-rewriteable groups are those whose derived groups have order 2. In the present paper, we shall ask the following question: how rewriteable can a finite group be if its derived group has order greater than 2? Formally, what is the maximum value of

$$\mathrm{Prw}_3(G) = \frac{\left|\{(x,y,z)\in G^3 \mid (x,y,z) \text{ is rewriteable}\}\right|}{|G|^3}$$

over all finite groups G such that $|G'| > 2$? Leavitt, Sherman and Walker have conjectured[**3**] that there is an upper bound strictly less than 1 for $\mathrm{Prw}_3(G)$ where G is not 3-rewriteable, and that 17/18 (achieved when G is S_3) is the best such bound. The main result of this paper confirms this conjecture:

THEOREM: *If G is a non-3-rewriteable group, then* $Prw_3(G) \leq 17/18$.

*Research funded by NSF grant #DMS-8922674

2. Some results on centralizers and conjugacy class sizes

The study of 3-rewriteability is, as one might expect, tightly bound up with the study of commutativity. Thus, we shall make extensive use of the centralizer subgroup. The centralizer of an element x will be denoted by $C(x)$. The centralizer of a subset S of a group will be denoted similarly, as C(S). The center of the group G will be called Z_G. The size of the conjugacy class containing x will be called $[x]$; this quantity is, of course, equal to $[G:C(x)]$. Finally, the expression $Pnrw_3(G)$ will be used to mean 1 - $Prw_3(G)$, or the probability that a randomly chosen triple is *not* rewriteable. We begin by restating a standard result.

Subgroup Intersection Inequality: *If K and L are subgroups of G,* $|K \cap L| \geq \frac{|K||L|}{|G|}$.

This is well known and I will not reproduce the proof here. Note that the inequality can also be expressed in terms of indices: that is, the index of the intersection of two subgroups is less than or equal to the product of their indices. From now on, we'll refer to this useful fact as the SI inequality. We call two subgroups S,T of G *independent* if the SI inequality is actually an equality; that is, the index of $S \cap T$ is equal to the product of the index of S and the index of T.

The proof of the main theorem depends largely on arguments on conjugacy class sizes. In general, our strategy will be to show that if any large conjugacy classes exist in a group, then many of the group's elements are in large conjugacy classes. Thus, many elements have small centralizers, few pairs of elements commute, and $Prw_3(G)$ is small. We begin with a result proved in [3]:

If x and y are elements of G for which [G:C(x)] = 2 and C(y)∩(G-C(x)) ≠ ∅, then [G:C(xy)] ≥ [G:C(y)].

Lemma 2.1 is a generalization of that result.

LEMMA 2.1: $[xy] \geq \frac{[G:C(x)\cap C(y)]}{min([x],[y])}$.

Proof. Apply the SI Inequality to C(xy) and C(x). Notice that C(xy)∩C(x) = C(<xy,x>) = C(<y,x>) = C(y)∩C(x). So

$$|C(y)\cap C(x)| \geq \frac{|C(xy)||C(x)|}{|G|}$$

$$|C(xy)| \leq \frac{|C(x)\cap C(y)||G|}{|C(x)}$$

$$=|C(x)\cap C(y)|[x].$$

Dividing both sides into the order of G gives

$$[xy] \geq \frac{[G:C(x)\cap C(y)]}{[x]}.$$

Since we chose x arbitrarily, we can assume without loss of generality that it has the larger centralizer of the two. The desired result follows.

We now present a pair of corollaries to Lemma 2.1.

COROLLARY 2.1a: $[xy] \geq \frac{max([x],[y])}{gcd([x],[y])}$ *for all x,y in G.*

Proof. C(x)∩C(y) is a subgroup of both C(x) and C(y). Therefore, its order is a divisor of the orders of both centralizers. Its index is consequently a multiple of both [x] and [y]. Now Lemma 2.1 tells us that

$$[xy] \geq \frac{lcm([x],[y])}{min([x],[y])}$$

which is equivalent to the form above.

COROLLARY 2.1b: *If x and y have independent centralizers, [xy] ≥ max([x],[y]).*

Proof. This follows directly from Lemma 2.1 with the appropriate substitution.

COROLLARY 2.1c: *If x and y do not commute, then* $[xy] \geq \frac{2\max([x],[y])}{\min([x],[y])}$

Proof. Without loss of generality we let $[x] \geq [y]$. Consider the index of $C(x) \cap C(y)$. This number is clearly a multiple of both $[y]$ and $[x]$. Can it be equal to $[x]$? No, because then $C(x)$ would be contained in $C(y)$, and x and y would commute. So the index of $C(x) \cap C(y)$ is at least $2[x]$. Substituting this into Lemma 2.1 yields the result.

With Lemma 2.1 and its corollaries in hand, we are ready to start discussing the conjugacy classes of the group as a whole. Our major result in this regard is Lemma 2.2.

LEMMA 2.2: *If G contains a conjugacy class whose size is a multiple of some prime p, then at least half the elements in the group are in conjugacy classes of size greater than or equal to p.*

Proof. Let x be an element such that p divides [x]. Now let Y be the set of all elements of G whose conjugacy classes have size less than p, and let y be some element of Y. We claim that $[xy] \geq p$. For $\max([x],[y]) = [x]$, which divides p, but $\gcd([x],[y])$ must divide $[y]$ and thus has no factor of p. So, by Corollary 2.1a, $[xy] \geq p$. Since this applies to any y in Y, we know that xY is disjoint from Y. So the cardinality of Y is at most half that of G. This proves the Lemma.

The final result of this section, Lemma 2.3, is admittedly rather *ad hoc*. It will, however, allow us in section 3 to eliminate from consideration any groups with conjugacy

classes of size 13 or greater. We introduce at this point the notation X_n; this refers to the subset of the elements of G in conjugacy classes of size n or greater.

LEMMA 2.4: *Suppose G contains a conjugacy class of size m>12. Then* $|X_6| \geq |Z_G| + \frac{m-1}{2m}|G|$.

Proof. Let Y be the set of non-central elements of G whose conjugacy classes are of size less than 6, and let x be an element such that $[x] = m$. How many elements of Y must be outside $C(x)$? $C(x)$ has order $|G|/m$, but $2|Z_G|$ of those are made up by the center itself and the coset xZ_G, neither one of which can be in Y. So at least $Y-|G|/m+2|Z_G|$ elements of Y lie outside $C(x)$. Let y be an element of Y that is not in $C(x)$. Suppose that $[y] = 2,3$, or 4. Then by Corollary 2.1c, $[xy] \geq 2m/[y] \geq 6$. Suppose $[y] = 5$. If $m \geq 15$, then Corollary 2.1c tells us that $[xy] \geq 6$. But if $12 < m < 15$, then m is not a multiple of 5, so Corollary 2.1a tells us that $[xy] \geq m \geq 6$. Therefore, each element of $Y - C(x)$ determines a distinct element of X_6. The coset xZ_G is also included in X_6, and has not yet been counted. So

$|X_6| \geq |Y| - |G|/m + 3|Z_G|$

$|X_6| \geq (|G| - |X_6| - |Z_G|) - |G|/m + 3|Z_G|$

$2|X_6| \geq (1 - 1/m)|G| + 2|Z_G|$, which gives the desired result.

3. The minimal counterexample M and its conjugacy classes

So far we've proved a number of facts about the sizes of conjugacy classes in finite groups, but we haven't yet related these facts to the problem at hand except in the vaguest

sense. Our next major result will provide an explicit lower bound for $Pnrw_3(G)$ based on the sizes of its conjugacy classes. First we'll need the following lemma:

LEMMA 3.1: *If $xzy \notin \{zyx,xyz,yzx\}$ and $zyx \neq xyz$, then at least one of the triples (x,z,y), (x,y,z), and (z,y,x) is not rewriteable.*

Proof. Suppose (x,z,y),(x,y,z), and (z,y,x) are all rewriteable. We know already that the product xzy does not equal zyx, xyz, or yzx. So it must be equal to either zxy or yxz.

Suppose $xzy = zxy$. Then x commutes with z, so $yxz = yzx$. Since (x,y,z) is rewriteable, xyz must equal either zxy, yzx, or yxz. But $xyz \neq xzy = zxy$, so $xyz = yzx$ or yxz. These two products are equal, so both must equal xyz. But this leaves no other permutation that can be equal to zyx, which contradicts the hypothesis that all three triples were rewriteable.

Now suppose $xzy = yxz$. What other permutation of the three elements can yield a product equal to zyx? Since $xzy \neq xyz$, y does not commute with z. So $zyx \neq yzx$. The only possibility remaining is zxy. But if $zyx = zxy$, x commutes with y and $xyz = yxz = xzy$. This contradicts the original stipulation that $xzy \neq xyz$. We conclude that at least one of the three stated triples is not rewriteable.

Armed with this result, we are ready to prove Proposition 1, which will provide a lower bound for $Pnrw_3(G)$.

PROPOSITION 1: $$Pnrw_3(G) \geq \frac{1}{3|G|} \sum_{\{g:[g]>3\}} \left(1 - \frac{1}{[g]}\right)\left(1 - \frac{3}{[g]}\right)$$

Proof. Choose some g in G whose conjugacy class contains more than 3 elements. Pick y which does not commute with g, and pick x such that

1) x does not commute with g

2) $y^{-1}x$ does not commute with g

3) yx does not commute with ygy^{-1}.

How many ways can we pick such x and y? There are clearly $|G| - |C(g)|$ possibilities for y. The three conditions on x require only that it be outside two cosets of $C(g)$ and one of $C(ygy^{-1})$. Both centralizers have the same order; thus, we know that there are at least $|G| - 3|C(g)|$ possibilities for x.

Now let $z = gy^{-1}$. We claim that the ordered triple (x,y,z) fulfills the condition of Lemma 3.1. Since y does not commute with g, it does not commute with z. So $xzy \neq xyz$. Since x does not commute with $g = zy$, we have $xzy \neq zyx$. Since $y^{-1}x$ does not commute with g, neither does $gy^{-1}x$ $(= zx)$. So $zxzy \neq zyzx$ and $xzy \neq zyx$. Finally, yx does not commute with $ygy^{-1} = yz$. So $yxyz \neq yzyx$ and $xyz \neq zyx$. This covers the four requirements. Therefore, one of the three triples (x,z,y), (x,y,z), (z,y,x) is non-rewriteable. Suppose we add the number of possible triples (g,x,y) for each g with conjugacy class size greater than 3. There will be at least $(|G|-|C(g)|)(|G|-3|C(g)|)$ such triples. It's clear that no non-rewriteable triple is counted more than 3 times by this method. Dividing this sum by 3 thus gives a lower bound for the number of non-rewriteable triples in G, and dividing further by $|G|^3$ results in the lower bound for $Pnrw_3(G)$ given above.

We will now turn our consideration to a group M, which we define to be a group of smallest order such that:

1) $|M'| > 2$ and

2) $Prw_3(M) > 17/18$.

The minimal counterexample approach will turn out to be very powerful in dealing with the problem of 3-rewriteability. We conclude this section by proving the following powerful constraint on M.

FACT 1: *No conjugacy class of M contains more than 8 elements.*

Proof. Suppose some conjugacy class has 12 or more elements. Then at least 11/24 of the elements of M have conjugacy class size at least 6, by Lemma 2.3. So by Proposition 1, $Pnrw_3(M) \geq (1/3)(11/24)(1-[1/6])(1-[3/6]) = 55/864 > 1/18$.

Suppose a conjugacy class has size 11. Then by Lemma 2.3, half the group has conjugacy class size at least 11. So $Pnrw_3(M) \geq (1/3)(1/2)(10/11)(8/11) = 80/726 > 1/18$.

The going gets more difficult when we consider a conjugacy class of size 10. By Lemma 2.2, X_5 makes up at least half the group. Proposition 1 tells us the following: if $[g] = 4$, g contributes at least $1/16|M|$ to $Pnrw_3$; if $[g] = 5$, g contributes at least $8/75|M|$ to $Pnrw_3$; and if $[g] = 10$, g contributes at least $21/100|M|$ to $Pnrw_3$. Recalling that X_5 contains X_{10}, and that X_4 contains both X_5 and X_{10}, we can state that

$$|M|Pnrw_3(M) \geq (1/16)|X_4| + (53/1200)|X_5| + (31/300)|X_{10}|.$$

We already know that half the group is in X_5, so this simplifies to

$$|M|Pnrw_3(M) \geq 53|M|/2400 + (1/16)|X_4| + (31/300)|X_{10}|.$$

If $Pnrw_3(M)$ is to be below 1/18, then $|X_4| \leq (241/450)|M|$. So if Y is the set of elements in conjugacy classes of size 2 or 3, then $|Y| \geq (209/450)|M|$. Now let x be an element in a conjugacy class of size 10, and let y be in $Y\text{-}C(x)$. By the argument used in the proof of Lemma 2.4, there are at least $|Y| - |M|/10 + 2|Z_M|$ such y. Substituting the known bound for $|Y|$ shows that there are at least $(82/225)|M|$ y in $Y\text{-}C(x)$. But Corollaries 2.1a and 2.1c imply that $[xy] \geq 10$. So $|X_{10}| \geq (82/225)|M|$. Combining this with the fact that $|X_4| \geq |X_5| \geq 1/2$ shows that $Pnrw_3(M) > 1/18$.

Finally, suppose that there is an element x in M whose conjugacy class contains 9 elements. Let Y be the set of elements whose conjugacy classes are of size 2,3,4, or 5.

There are at least $|Y| - |M|/9 + 2|Z_M|$ elements in Y-C(x); if y is such an element, then Corollaries 2.1a and 2.1c imply that $[xy] \geq 6$. So

$$|X_6| \geq |Y| - |M|/9 + 2|Z_M|$$

$$|X_6| \geq (|M| - |X_6| - |Z_M|) - |M|/9 + 2|Z_M|$$

$$|X_6| \geq 4|M|/9.$$

Thus, by Proposition 1, $Pnrw_3(M) \geq (4/9)(5/36) = 5/81 > 1/18$. So the fact is true as claimed.

FACT 2: *M has no conjugacy class with 7 elements.*

Proof. By Lemma 2.1, if M has a conjugacy class of size 7 at least half the elements of M are in conjugacy classes of size 7 or larger. This implies that $Pnrw_3(M) \geq (1/3)(1/2)(24/49) > 1/18$.

We'll also need to eliminate the possibility of conjugacy classes of size 5. This is a little more difficult. For now, we'll content ourselves with proving the following lemma.

FACT 3: *If M contains a conjugacy class of size 5, then $|M'| = 5$.*

Proof. First, we'll show that no conjugacy class in M has size greater than 5. Suppose $[x] > 5$. Then $[x]$ equals 6 or 8. Both of these are relatively prime to 5. So, by Lemma 2.1, if $[y] = 5$, $[xy] > 5$. This implies that at least half the elements of X_5 have conjugacy class size *strictly* greater than 5; that is, they're in X_6. Lemma 2.2 tells us that X_5 covers at least half of M. So by Proposition 1, $Pnrw_3(M) \geq (1/4)(8/75) + (1/4)(5/36) > 1/18$. Thus, 5 is the maximum size of any conjugacy class in M. Wiegold [4] has shown that if the maximum conjugacy class size in a group is some prime p, then the derived group has order p. This is exactly the desired result.

4. A combinatorial formula for $Prw_3(G)$

In this section we will derive an explicit formula for $Prw_3(G)$ using several parameters of combinatorial group theory. The formula is the following:

PROPOSITION 2: $Prw_3(G) = \frac{5k - 8\beta + 4t}{|G|}$, *where k is the number of conjugacy classes of G, β is the sum of the reciprocals of the conjugacy class sizes, and t is the number of mutually commutative ordered triples divided by $|G|^2$.*

Proof. By the Principle of Inclusion and Exclusion, the number of ordered triples which are rewriteable can be expressed as

$$\sum_{P \subset S_3 - \{1\}} (-1)^{|P|+1} N(P)$$

where P is some subset of the nontrivial permutations of three elements and N(P) is the number of ordered triples (x,y,z) whose product is invariant under all the permutations in P. The actual application of the PIE is tedious but straightforward; I will present three representative examples to indicate how each of the three parameters in the formula arises. Suppose P is the single permutation $(x,y,z) \dashrightarrow (x,z,y)$. Then N(P) is just the number of ordered triples (x,y,z) such that y and z commute. By Erdös's result in [3], there are $k|G|$ such y and z. Since x can be chosen arbitrarily, $N(P) = k|G|^2$. Now consider the case where P consists of the two permutations taking (x,y,z) to (x,z,y) and (y,x,z) respectively. If a triple is to maintain its product under both these permutations, then x and z must both commute with y. So N(P) can be expressed as the sum over all y in G of $|C(y)|^2$. But notice that this sum evaluated over any conjugacy class is $[y]|C(y)|^2 = |G|^2/[y]$. So the sum

over G is just ß$|G|^2$. In fact, another useful definition of ß is $\frac{1}{|G|^2}\sum_{x\in G}|C(x)|^2$. Finally, suppose that P comprises all non-trivial permutations of (x,y,z). Then if the product is to remain invariant under P, x, y, and z must be mutually commutative. By definition, $N(P) = t|G|^2$.

It is interesting to define a series a_n as follows:

$$a_n = \frac{1}{|G|^n}\sum_{x\in G}|C(x)|^n$$

Then $a_0 = |G|$, $a_1 = k$, and $a_2 = ß$. We shall meet a_3, or γ, in section 6.

5. The normal subgroups of M

We've derived a good deal of information based on the fact that M is a counterexample to the theorem; that is, that $Prw_3(M) > 17/18$. But so far we've ignored the fact that M is a *minimal* counterexample. As it turns out, this stipulation will be of crucial importance. The use of a minimal counterexample suggests a descent method; that's exactly what we'll do in the following lemma and proposition.

LEMMA 5.1: *If N is a normal subgroup of G, then* $Prw_3(G/N) \geq Prw_3(G)$.

Proof. Let f be the natural homomorphism from G to G/N. Let (x',y',z') be a non-rewriteable triple in G/N. Then if $x\in f^{-1}(x')$, $y\in f^{-1}(y')$, and $z\in f^{-1}(z')$, the triple (x,y,z) is non-rewriteable in G. For if the product xyz is invariant under some nontrivial permutation, then $f(x)f(y)f(z) = x'y'z'$ is clearly invariant under the same permutation. The

inverse image of any element in G/N has cardinality |N|. So each non-rewriteable triple in G/N corresponds to $|N|^3$ non-rewriteable triples in G. Therefore,

$$\mathrm{Pnrw}_3(G) = \frac{\left|\{(x,y,z)\in G^3 \mid (x,y,z) \text{ is non-rewriteable}\}\right|}{|G|^3}$$

$$\geq \frac{|N|^3\left|\{(x',y',z')\in G/N \mid (x',y',z') \text{ is non-rewriteable}\}\right|}{|G|^3}$$

$$= \mathrm{Pnrw}_3(G/N).$$

The inequality is not in general an equality because it's quite possible for non-rewriteable triples in G to have rewriteable images under f.

Now we're ready to prove a strong result on the quotient groups of M.

FACT 4: *Every proper quotient group of M is 3-rewriteable.*

Proof. Consider a quotient group M/K. By Lemma 5.1,

$$\mathrm{Prw}_3(M/K) \geq \mathrm{Prw}_3(M) > 17/18.$$

So if M/K is not 3-rewriteable, it is a counterexample to the Theorem. But |M/K| is smaller than |M|, and M is a minimal counterexample. This is a contradiction.

COROLLARY 4a: *If K is a proper normal subgroup of M, then $|K\cap M'|$ is either $|M'|$ or $(1/2)|M'|$.*

Proof. Recall that a 3-rewriteable group has derived group of order 1 or 2. So if K is normal in M, we know by Fact 4 that |(M/K)'| is 1 or 2. It is well known that if N is a normal subgroup of G, (G/N)' = G'N/N. So

$$|(M/K)'| = \frac{|M'K|}{|K|} = \frac{|M'||K|}{|M'\cap K||K|} = \frac{|M'|}{|M'\cap K|}.$$

Since this quantity is either 1 or 2, the corollary is true as desired.

6. M has trivial center

We've now established all the machinery we need to begin placing some serious structural restrictions on M. We'll start by proving that M is not a p-group. First, suppose $p \geq 5$. Then the desired contradiction follows directly from Proposition 1. For $|Z_M| \leq (1/25)|M|$, so at least $(24/25)|M|$ elements are in conjugacy classes of size 5 or greater. Thus,

$$Pnrw_3(G) \geq (1/3)(24/25)(8/25) = 192/1875 > 1/18.$$

Therefore, if M is a p-group, p equals 2 or 3. Suppose p=3. Then M' is also a 3-group. By Corollary 4a, any normal subgroup of M contains at least half of M'. But it's well-known that every p-group contains a normal subgroup of order p; thus, we may choose K normal in M with $|K| = 3$. So it's clear that $|M'|$ must equal 3 as well. What if p=2? Then there's a normal subgroup K of M with $|K| = 2$. So $|M'| = 2$ or 4. But if $|M'| = 2$, then M is itself rewriteable and need not be considered. So we're left with two cases:

i) M is a 3-group, $|M'| = 3$.

ii) M is a 2-group, $|M'| = 4$

In order to eliminate these cases, we'll have to introduce the parameter γ, which we defined at the end of section 4.

We can transform the definition given for γ as follows:

$$\gamma = \frac{1}{|G|^3} \sum_{x \in G} |C(x)|^3$$

$$= \frac{1}{|G|^3} \sum_{x \in G} \sum_{y \in C(x)} |C(x)|^2$$

$$= \frac{1}{|G|^3} \sum_{x \sim y} |C(x)|^2$$

$$= \frac{1}{|G|^3} \sum_{x \sim y} (1/2)|C(x)|^2 + (1/2)|C(y)|^2$$

$$= \frac{1}{2|G|^3} \sum_{x \sim y} (|C(x)|^2 + |C(y)|^2),$$

where $x \sim y$ denotes the sum over all ordered commuting pairs (x,y). It will turn out to be useful to compare γ with t. Recall that $t = (1/|G|^2)T$, where T is the total number of mutually commutative ordered triples (x,y,z) in G. So we can write

$$t = \frac{1}{|G|^2} \sum_{x \sim y} |\{z: z \text{ commutes with both } x \text{ and } y\}|$$

$$= \frac{1}{|G|^2} \sum_{x \sim y} |C(x) \cap C(y)|$$

$$= \frac{1}{2|G|^3} \sum_{x \sim y} 2|G||C(x) \cap C(y)|.$$

Therefore,

$$\gamma - t = \frac{1}{2|G|^3} \sum_{x \sim y} |C(x)|^2 - 2|G||C(x) \cap C(y)| + |C(y)|^2.$$

We will denote the summand of the right-hand side by $D(x,y)$. It will be simpler to consider the sum of $D(x,y)$ over all pairs that do *not* commute than over those that do. The

two sums are simply additive inverses, however. For the sum of the squared centralizer orders of the elements of G is ß|G|^2, by definition of ß. So the sum of the squared centralizer order of x over all pairs (x,y) is ß|G|^3, since y is chosen arbitrarily. But the sum of $|C(x)\cap C(y)|$ over all pairs x,y is just the same as counting the number of pairs (x,y) which both commute with z over all z in G. The number of such pairs is just $|C(z)|^2$, so this sum too is equal to ß|G|^2. So the sum of $D(x,y)$ over *all* pairs (x,y) is just ß|G|^3 - 2ß|G|^3 + ß|G|^3 = 0.

The function $D(x,y)$ seems somewhat arcane. However, we will be able to show that for certain special classes of groups, the sum of D over all commuting pairs is positive, thereby bounding t above by γ.

LEMMA 6.1: *If G is a p-group and $|G'| = p$, then $\gamma = t$.*

Proof. Suppose x and y are two element in G which do not commute. Then both x and y are non-central, so $[x] = [y] = p$. Since x and y do not commute, their centralizers do not coincide. Thus, $|C(x)\cap C(y)| = (1/p^2)|G|$. So it's clear that $D(x,y) = 0$. Since the sum of D over all non-commuting pairs is 0, the sum over commuting pairs is 0 as well. So $\gamma = t$.

In fact, a simple modification to this argument is enough to show that if all the conjugacy classes in a group have prime size, then $\gamma \geq t$.

LEMMA 6.2: *If G is a 2-group and $|G'| = 4$, then $\gamma \geq t$.*

Proof. Once again, suppose x and y do not commute. We can separate all such pairs of elements into the following cases, using the SI inequality:

$[x]$	$[y]$	$[G:C(x)\cap C(y)]$	$D(x,y)$
2	2	4	0
2	4	8	(1/16)|G|
4	2	8	(1/16)|G|

4	4	8	(-1/8)|G|
4	4	16	0

Suppose (x,w) is a non-commuting pair of elements in G such that $[x] = 2$, $[w] = 4$, and $[G:C(x)\cap C(w)] = 8$. Each such pair (x,w), along with (w,x), contributes $(1/8)|G|$ to the sum over all non-commuting pairs of $D(x,w)$. Consider the pair of elements (w,xw). Since w and x have independent centralizers, Corollary 2.1b tells us that $[xw] = 4$. Now $C(w)\cap C(xw) = C(w)\cap C(x)$, which has index 8. Thus, the pair (w,xw) contributes $(-1/8)|G|$ to the sum. Since each pair (x,w) generates a unique (w,xw), and since the former are the only pairs that can make a positive contribution to the sum, we conclude that the sum over all non-commuting pairs of D is non-positive, and thus that $\gamma \geq t$.

Testing indicates that the following stronger result holds: If G is a p-group and $|G'| = p^2$, then $\gamma = t$. The inequality $\gamma \geq t$ seems to hold for almost all groups; large dihedral groups, for instance, are exceptions.

With Lemmas 6.1 and 6.2 we've covered exactly those cases that were still admissible for our minimal counterexample M. So we know that $\gamma \geq t$. Combining this fact with Proposition 2 gives

$$\mathrm{Prw}_3(M) \leq \frac{5k - 8\beta + 4\gamma}{|M|}. \text{ Therefore,}$$

$$\mathrm{Pnrw}_3(M) \geq \frac{1}{|M|}(|M| - 5k + 8\beta - 4\gamma)$$

$$= \frac{1}{|M|}\sum_{x \in M} 1 - 5\left(\frac{|C(x)|}{|M|}\right) + 8\left(\frac{|C(x)|}{|M|}\right)^2 - 4\left(\frac{|C(x)|}{|M|}\right)^3$$

$$= \frac{1}{|M|} \sum_{x \in M} \left(1 - \frac{|C(x)|}{|M|}\right)\left(1 - 2\frac{|C(x)|}{|M|}\right)^2$$

If M is a 3-group, then at least (8/9)|M| elements are in conjugacy classes of size 3 or more, so $Pnrw_3(M) \geq (8/9)(2/27) = 16/243 > 1/18$. Suppose M is a 2-group, and let w be an element whose conjugacy class has size 4. (It is not difficult to show that if there is no such element, M' has order 2.) Then by Corollary 2.1c, if $[x] = 2$ and x does not commute with w, then $[xw] = 4$. Thus, of the (3/4)|M| elements outside $C(w)$, at least half are in conjugacy classes of size 4 or greater. So $Pnrw_3(M) \geq (3/8)(3/16) = 9/64 > 1/18$.

FACT 5: *M is not nilpotent.*

Proof. We've now shown that M is not a p-group. Suppose M is some nilpotent group which is not a p-group. Then M is the direct product of its Sylow p-subgroups. Since these p-subgroups are isomorphic to proper quotient groups of M, they must be 3-rewriteable. Any 3-rewriteable group of odd order must clearly be Abelian, since the derived group cannot have order 2. So all the Sylow p-groups of M with p>2 are Abelian. Thus, we can write M as $T \times A$, where T is the 3-rewriteable Sylow 2-group of M and A is the (Abelian) direct product of the other Sylow p-subgroups. Such a group is clearly itself 3-rewriteable; since we defined M to be non-3-rewriteable, this is a contradiction and M cannot be nilpotent.

FACT 6: *M has trivial center.*

Proof. Suppose Z_M is non-trivial. Then M/Z_M is a proper quotient group of M and is thus 3-rewriteable. Now start with the group M/Z_M and keep taking central quotients until we reach either the identity or another group with trivial center. By Lemma

5.1, any quotient group of a 3-rewriteable group is itself 3-rewriteable. So the end result of this process is a 3-rewriteable group with trivial center. Since we've shown that M is not nilpotent, the series of central quotients cannot lead to the identity. So the group in question is a non-trivial center-free 3-rewritable group. In fact, no such group exists. For a non-Abelian 3-rewriteable group has even order (since the commutator subgroup has order 2) and all the non-central conjugacy classes are of even size-- namely, order 2. So the size of the center must also be even. We conclude that our initial supposition was incorrect, and that M has trivial center.

FACT 7: *M has no conjugacy class of size 5.*

Proof. Assume the contrary is the case. Then, by Lemma 3.2, $|M'| = 5$. As before, call the 5-Sylow subgroup F. Since the derived group of M is abelian, M is solvable; thus, M has a Hall subgroup whose order is [M:F]. Call that subgroup H. Now H is disjoint from M', since 5 doesn't divide |H|. So H is abelian. Let $D = C(F) \cap H$. Suppose D is non-trivial, and let d be a non-identity element of D. Then D commutes with all of F and all of H, so it commutes with their product HF. But this product is clearly equal to all of M, so d is central. This is a contradiction; therefore, we can assume that D is trivial. I claim that the index of C(F) is 2. Suppose the index of C(F) is greater than 2, and let x be some element which does not commute with F. Then F clearly induces at least 5 conjugates of x, so x is in X_5. So at least 2/3 of M is in X_5. But this means that $Pnrw_3(M) \geq (2/3)(8/75) = 16/225 > 1/18$, a contradiction. Now the index of C(F) is 2 and the index of H is |F|; thus, the index of D is no more than 2|F|. We conclude that $|M| \leq 2|F|$. Since M can't be a p-group, $|M| = 2|F|$. Since $|C(F)| = |F|$, F is abelian. Now let a be an element not in F. If a commutes with some f in F, then $C(f)$ includes both F and aF; that is, the whole group. Since M is center-free, this means that f is the identity. But $C(a)$ has index 5. So if $C(a)$ is disjoint from F, $|F|=5$. So $M = D_5$, which is easily seen to satisfy $Prw_3(M) > 17/18$.

7. M is a 2,3-group and M' is a 2-group

We've now shown that all the conjugacy classes of M are of size 1,2,3,4,6, or 8. Notice that these possibilities have only 2 and 3 among their prime factors. The following Lemma will allow us to make use of this fact.

LEMMA 7.1: *If a prime p divides $[G:Z_G]$, then p divides $[x]$ for some x in G.*

Proof. Suppose p does not divide $[x]$ for any x in G. Then for every x, $|C(x)|$ contains as many factors of p as does $|G|$. Thus, a Sylow p-subgroup of $C(x)$ is also a Sylow p-subgroup of G. Choose one such subgroup and call it S_p. Since all Sylow p-subgroups of G are conjugate to S_p, we can restate the hypothesis as follows: For each x in G, $C(x)$ contains a conjugate of S_p. This is clearly equivalent to stating that x is contained in some conjugate of $C(S_p)$. Therefore, the union of all the conjugates of $C(S_p)$ must be the whole group. (Note that p divides $[G:Z_G]$, so S_p is not central and $C(S_p)$ is not itself the whole group.) We claim that this union cannot in fact cover the whole group. Let $C_p = C(S_p)$; then we have

$$\left| \bigcup_{g \in G} (C_p)^g \right| \leq |C_p|[G:N_G(C_p)] \leq |C_p|[G:C_p] = |G|.$$

The leftmost inequality has an equality case only when the conjugates are pairwise disjoint. But since the identity is in each conjugate, such is not the case and the inequality is strict. Thus, the union of the conjugates of C_p does not cover the whole group, and there is an conjugacy class in G whose size is a multiple of p.

FACT 8: *M is a 2,3-group*

Proof. We know that no prime other than 2 or 3 divides the size of any conjugacy class in M. So $[M:Z_M] = 2^a3^b$, by the lemma above. But the center of M is trivial. So M is a 2,3-group.

FACT 9: *M' is a 2-group.*

Proof. We begin by considering minimal normal subgroups of M. If K is a minimal normal subgroup and N is a normal subgroup, it is clear that $K \cap N$ is either trivial or equal to K. Recall that by Corollary 4a, $|K \cap M'| \geq (1/2)|M'|$. Since $|M'| > 2$, we conclude that every minimal normal subgroup is contained in M' and has at least half the order of M'.

Any minimal normal subgroup must clearly be characteristic-free. It is well known (see Robinson [5], for instance) that characteristic-free groups are direct products of isomorphic copies of a simple group. But K is a 2,3-group, and is thus solvable. So the simple group that makes up K must be either Z_2 or Z_3, and K is an elementary Abelian 2- or 3-group. In fact, K is a 2-group, as will be shown by the following lemma.

LEMMA 7.2: *If a group G has a normal subgroup H which is isomorphic to $(Z_3)^n$, $n \geq 2$, and which is disjoint from the center of G, then 9 divides the size of some conjugacy class in G.*

Proof. Suppose the opposite is true. Consider G as a group of automorphisms of H. Then each automorphism in G fixes at least 1/3 of the elements of H. Since H intersects Z_G trivially, the automorphisms in G cannot all have the same fixed-point-set in H. Let x and y be elements of G-C(H) which fix different sets of points in H, and let F_x and F_y be these sets (which are also subgroups of H.) Let K be the quotient group $H/(F_x \cap F_y)$; since $F_x \cap F_y$ is fixed under conjugation by $\langle x,y \rangle$, we can consider the action of $\langle x,y \rangle$ on K by conjugation. K is isomorphic to $Z_3 \times Z_3$. So we're dealing with a somewhat simpler situation. <x,y> defines a group of automorphisms of $K \cong Z_3 \times Z_3$ with the following properties: each automorphism fixes at least 1/3 of K, and among the fixed-point sets of the automorphisms are two *distinct* proper subgroups of K [corresponding to F_x and F_y.] It is easy to verify that no such automorphism group on $Z_3 \times Z_3$ exists, thus proving the lemma.

Since we've already shown that no conjugacy class in M has size a multiple of 9, the lemma implies that K is either a 2-group or is isomorphic to Z_3. Suppose the latter is the case. Then by Corollary 4a, there are only three possibilities for the structure of M':

i) $M' \cong Z_3$

ii) $M' \cong Z_3 \times Z_2$

iii) $M' \cong S_3$

The latter two cases are easy, so we'll deal with them first. Suppose $M' \cong Z_3 \times Z_2$ and x is the element of order 2 in M'. Then $\langle x \rangle$ is clearly a normal subgroup of M which covers less than half of M'. As for case iii, it turns out that there are no groups with derived group isomorphic to S_3. Dixon's argument [2] that no group has a derived group isomorphic to S_4 suffices to prove the result we need.

Suppose $M' \cong Z_3$. Denote the elements of M' by $\{e,x,x^2\}$. Since M is center-free, the set $\{x,x^2\}$ must be a conjugacy class; thus, $|C(x)| = |C(M')| = (1/2)|M|$. Now choose an element a outside C(M'), and consider its centralizer C(a). What is the size of a's

conjugacy class? The only elements that can be conjugate to a are a itself, ax, and ax^2. But if all three of these elements are not in the same conjugacy class, then at least one of them must be in its own conjugacy class. Since M is center-free, this is impossible. So $[a] = 3$ and $|C(a)| = (1/3)|M|$. Furthermore, $[C(a)]' \subset C(a) \cap M' = \{e\}$, since we picked a not to commute with x. So $C(a)$ is abelian. Now let D be the intersection of $C(a)$ with $C(M')$. Since the former subgroup has index 3 in M and the latter has index 2, D has index 6. We will suppose that $|M| > 6$; otherwise, $M \cong S_3$, which is easily determined to have Prw_3 equal to 17/18. Thus, D is non-trivial; let d be some element in D other than the identity. Then $C(d)$ certainly includes $C(a)$ and M'. But then it must also include their product $C(a)M'$. Since the two subgroups are disjoint, the order of their product is the product of their orders; that is, $|M|$. So d is central, which violates the requirement that M be center-free. We conclude that M' is not isomorphic to Z_3, and furthermore that K is a 2-group. Since [M':K] equals 1 or 2, M' is a 2-group as well. We are now ready for the final portion of the proof.

8. Proof of the Theorem

We've now established that M is a center-free 2,3-group whose derived group is a 2-group. This information will be enough to attack and eliminate this case directly. First, however, we need some lemmas regarding the structure of M. From now on, A will refer to some 3-Sylow subgroup of M, and B to the 2-Sylow subgroup (which is normal by virtue of containing M').

FACT 10: *A is abelian.*

Proof. Immediate, since A is disjoint from M'. If x and y are in A, then their commutator is in both A and M' and is thereby trivial.

FACT 11: $C(B) \subset B$.

Proof. First, note that A is disjoint from C(B). For suppose a nontrivial element a is in both subgroups. Then C(a) contains both A and B. But since |A||B| = |M| and A and B intersect trivially, their product is the whole group. This implies that a is central, a contradiction.

Now C(B) is the centralizer of a normal subgroup and is thus itself normal. So the product AC(B) is a subgroup of M whose order is |A||C(B)|, since we've just shown the intersection of the two subgroups to be trivial. Since |A| contains all the factors of 3 that are in |M|, C(B) must be a 2-group, and is thus contained in B.

We'll now introduce the subgroup D, which is the normal core of the centralizer of A. D can also be expressed as:

The intersection of all conjugates of the centralizer of A

The intersection of the centralizers of all the conjugates of A

The set of all elements which commute with each 3-Sylow subgroup of M.

We will show that D is trivial. Suppose the opposite is true. Then D is a non-trivial normal subgroup and hence contains K. Therefore, $K \subset D \subset C(A)$.

Consider the quotient group M/K. This is 3-rewriteable, so by the result of [2] it can be expressed as $T \times F$, where T is a 2-group and F is abelian. Since K is a 2-group, it's clear that F is an isomorphic image of A. Since F is in the center of M/K, the commutator subgroup [F,M/K] is trivial. Mapping back out to the original group, we conclude that $[A,M] \subset K$. So $[A,M] \subset C(A)$.

Choose an element a in A whose order is 3, and an arbitrary element m in M. Then

$[a,m]^3$

$= [a,m]^2 ama^{-1}m^{-1}$

$= [a,m]a[a,m]ma^{-1}m^{-1}$

$= [a,m]a^2ma^{-2}m^{-1}$

$= a^2[a,m]ma^{-2}m^{-1}$

$= a^3ma^{-3}m^{-1}$

$= [a^3,m] = [e,m] = e.$

So $[a,m]$ has order 3. But $[a,m]$ is in M', which is a 2-group; thus, $[a,m] = e$ for arbitrary m in M. But this means that a is central, which is impossible. So D is trivial.

Using the third formulation for D, we can then say that for every non-identity element m of M, there is a 3-Sylow subgroup A of M which does not commute with m. Such a subgroup clearly induces at least 3 conjugates of m. So all the non-trivial conjugacy classes of M have size 3 or greater. Furthermore, if m is not in B, then B is not contained in $C(m)$ by Fact 11. So $|C(m)|$ must have at least one fewer factor of 2 than |M| does. In other words, the size of any conjugacy class outside B is even, and thus at least 4. Suppose $|A| \geq 9$. Then at least 8/9 of M is in conjugacy classes of size 4 or greater, from which Proposition 1 gives $Pnrw_3(M) \geq (8/9)(1/16) = 1/18$.

So $|A| = 3$. We claim also that B is abelian; if it's not, then at least (3/4)|B| is outside C(B) for a total of (11/12)|M| elements in conjugacy classes of size 4 or greater, which pushes $Pnrw_3$ above 1/18 once again. Let a be a nontrivial element of A. Any element of B which commutes with a must be central, since it commutes with all of B and all of A. So $C(a)$ is disjoint from B. Therefore, the product $BC(a)$ has order $|B||C(a)|$. Since this order is less than |M|, we conclude that $[a] = [M:C(a)] \geq |B|$. Since $|M'| \leq |B|$, we conclude that $[a]$ equals |B| exactly. So 2/3 of the group is contained in two conjugacy classes or order |B|, one containing a and the other containing a^2. Suppose $|B| \geq 8$. Then by Proposition 1, $Pnrw_3(M) \geq (2/3)(35/192) > 1/18$.

So $|B| \leq 4$. It's easy to check that the only possibility remaining is A_4, and that $Prw_3(A_4) \leq 17/18$. This completes the proof of the Theorem.

References

1. M. Curzio, P. Longobardi and M. Maj, *Su di un problema combinatorio in teoria dei gruppi*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. 74 (1983), 136-142.

2. J.A. Dixon, **Problems in Group Theory**, Blaisdell, 1967.

3. J.L. Leavitt, G.J. Sherman and M.E. Walker, *Rewriteability in Finite Groups*, Amer. Math. Monthly (to appear).

4. J. Wiegold, *Groups with boundedly finite classes of conjugate elements.* Proc. Roy. Soc. London Ser. A. 238 (1957), 389-401.