8-1992

Some Upper Bounds for Commutativity and Cyclicity Measures in Finite Groups

David Patrick
Carnegie Mellon University

Catherine Sugar
Pomona College

Eric Wepsic
Harvard University

SOME UPPER BOUNDS FOR COMMUTATIVITY AND CYCLICITY MEASURES IN FINITE GROUPS

D. Patrick, C. Sugar and E. Wepsic

MS TR 92-06

August 1992

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

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

Some Upper Bounds For Commutativity And Cyclicity Measures In Finite Groups

David Patrick * Catherine Sugar * Eric Wepsic *

August 4, 1992

1 Introduction

The idea of commutativity is fundamental to almost every area of mathematics. Because the first mathematical sets that one encounters, such as the integers and the real numbers, are commutative under all the standard operations, we tend to take commutativity for granted, and do not realize how special and useful a property it is. One of the first places that non-commutative sets are encountered is in Abstract Algebra, in the field of Group Theory. Since a group is simply a set together with an operation with specific properties, it is natural that commutativity should be an important topic in group theory. There is, of course, a special term for a group in which each element commutes with every other element. Such a group is called *abelian.* Abelian groups are well understood because they are very well-structured. However, most groups are not abelian. This begs the following questions: (1) How commutative can a non-abelian group be? and (2) Is there some way of quantifying the abelian-ness of groups? The answer to the second question is certainly yes. For instance, it is well known that for a non-abelian finite group, the probablility that two randomly chosen group elements will commute is less than or equal to 5/8. It turns out that for finite groups there are several useful quantitative measures of abelian-ness. Therefore, for the remainder of this paper, we will restrict our attention to finite groups.

As indicated above, one measure of the abelian-ness of a finite group is what fraction of pairs of group elements commute with each other. There

*Work supported by NSF grant number DMS-910059

are many ways to generalize this idea. One important such generalization is the idea of rewritability. A group is n-rewritable if for every ordered n-tuple of group elements $(x_1, x_2, \ldots, x_n)$ there exists some non-trivial $\sigma \in S_n$ such that

$x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$.

A group is abelian iff for every ordered n-tuple of group elements, $x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ for every $\sigma \in S_n$. (For more information on rewritability and rewritable groups, see [2].) For the generalization with which this paper is primarily concerned, the following definition is useful:

DEFINITION: If G is a finite group, then an n-tuple, $(x_1, x_2, \ldots, x_n)$, is called a **mutually commuting n-tuple** if $x_i x_j = x_j x_i$ for all $1 \leq i, j \leq n$.

The percentage of n-tuples of a group G which are mutually commuting is another measure of the group's abelian-ness. Note that a group is abelian iff every ordered n-tuple of elements is mutually commuting. In [1], Erdös and Strauss found a lower bound for the number of mutually commuting n-tuples in a finite non-abelian group, thus implying that a group has at least some minimal amount of commutativity. Yet another measure of commutativity is the probability that n elements of a finite group generate a cyclic subgroup. It is easy to see that if an n-tuple generates a cyclic subgroup, then that n-tuple is mutually commuting. In this report we find a sharp upper bound for the number of mutually commuting n-tuples in a finite group, and show that this bound also applies to the number of n-tuples which generate a cyclic subgroup.

2 Mutually Commuting n-Tuples In A Finite Group

The main purpose of this section is to find an upper bound for the number of mutually commuting n-tuples in a finite group, G. Before we proceed with the exposition of this result, it will be useful to have the following notation. For $n \geq 2$

$$\mathrm{Pr}_n\mathrm{Com}((G)) = \frac{|\{(x_1, x_2, \ldots, x_n) \in G^n : x_i x_j = x_j x_i, 1 \leq i, j \leq n\}|}{|G|^n}$$

Thus, $PrCom2(G)$ is the probability that two elements of group G commute. The following fact, stated earlier, has been known for a long time and its proof is worth looking at briefly:

FACT 1: For G a finite non-abelian group, Pr-2Com(G) $\leq 5/8$, and furthermore, this bound is achieved iff $G/Z \cong Z_2 \times Z_2$.

Proof: Assume $G/Z \cong Z_2 \times Z_2$. Then $|Z| = |G|/4$ and G can be written as a union of four distinct cosets of the center, $G = Z \cup wZ \cup xZ \cup yZ$. Note that if $a, b \in wZ$ then $a = wz_1$ and $b = wz_2$ where $z_1, z_2 \in Z$. Thus $ab = wz_1wz_2 = wwz_1z_2 = wwz_2z_1 = wz_2wz_1 = ba$. Thus for $a \in wZ, C(a) = Z \cup wZ$ and $|C(a)| = |G|/2$. In fact if a is not in the center of $G, C(a) \leq 1/2$ for any group G since the centralizer is a subgroup.

Now suppose a and b commute. Then either a is in the center or it isn't. The probability that a is in the center is 1/4. In this case any b will commute with a, so a quarter of the pairs in $G \times G$ are of this form.

Suppose a is not inthe center. The probability of this happening is 3/4. From above, the probability that $b \in C(a)$ is 1/2. Thus the probability of getting a commuting pair of this type is $(3/4)(1/2) = 3/8$. Adding the probabilities for the two cases gives us $Pr_2Com(G) = 5/8$.

Now suppose $G/Z \ncong Z_2 \times Z_2$. It is well known that if G/Z is cyclic, G is abelian. Since we are only considering non-abelian G, this tells us that G/Z is not of prime order, 2,3, etc., nor is it isomorphic to the cyclic group of order 4. Since the only other group of order less than or equal to 4 is $Z_2 \times Z_2$, by our assumption $|G/Z| > 4$ and hence $|Z|/|G| < 1/4$. If we let $f = |Z|/|G|$ then again splitting the set of commuting pairs (a, b) into the cases where a is or is not in the center, we get $Pr_2Com(G) \leq f + (1/2)(1-f) < (1/2) + (1/2)(1/4) = 5/8$. $\square$

We are now ready to prove the main result of this section:

THEOREM 2: Let G be a finite, non-abelian group. Then

$$Pr_nCom(G) \leq (1/2)^n[3 - (1/2)^{n-1}]$$

Furthermore, equality obtains iff $G/Z \cong Z_2 \times Z_2$.

Proof: The proof is by induction on n. By FACT 1, the result holds for $n = 2$. Now assume the result holds for $n - 1$.

We first show that equality obtains if $G/Z \cong Z_2 \times Z_2$:

Let $(x_1, x_2, \ldots, x_n)$ be a mutually commuting n-tuple. There are two possible cases.

CASE 1: x_1 is in the center of G. Since $G/Z \cong Z_2 \times Z_2$

the probability of this occuring is $1/4$. In this case all that is necessary is that $(x_2, x_3, \ldots, x_n)$be a mutually commuting $(n-1)$-tuple. By the induction hypothesis, the probability of this is $(1/2)^{n-1}[3-(1/2)^{n-2}]$. Thus the probability of getting a mutually commuting n-tuple with the first element in the center is given by

$$Prob(Case1) = (1/4)(1/2)^{n-1}[3-(1/2)^{n-2}] = 3(1/2)^{n+1} - (1/2)^{2n-1}$$

CASE 2: x_1 is not in the center of G. The probability of this occuring is $3/4$. In this case we must have $x_2 \in C(x_1)$. As discussed in the proof of FACT 1, this has probability $1/2$. We must also have x_3 commute with x_1 and x_2 and so forth. By the argument in the proof of FACT 1, it will be sufficient to have $x_3, x_4, \ldots, x_n$ in the centralizer of x_1. For each of $x_2, \ldots, x_n$ this probability is $1/2$. Thus the probability of getting a mutually commuting n-tuple with the first element not in the center is

$$Prob(Case2) = (3/4)(1/2)^{n-1} = 3(1/2)^{n+1}.$$

From this we conclude that

$$\begin{aligned} Pr_nCom(G) &= Prob(Case1) + Prob(Case2) \\ &= 3(1/2)^{n+1} - (1/2)^{2n+1} + 3(1/2)^{n+1} \\ &= 3(2)(1/2)^{n+1} - (1/2)^n(1/2)^{n-1} \\ &= (1/2)^n[3-(1/2)^{n-1}] \end{aligned}$$

and the result is proved.

Now it only remains to show that $Pr_nCom(G)$ is strictly less than $(1/2)^n[3-(1/2)^{n-1}]$ for groups with $G/Z \ncong Z_2 \times Z_2$. We proceed in exactly the same way as in the proof of FACT 1. Let $f = |Z|/|G|$. Then we have that:

i) Prob(Case 1) $= f(Pr_nCom(G)) \leq f(1/2)^{n-1}[3-(1/2)^{n-2}]$,

ii) Prob(Case 2) $\leq (1-f)(1/2)^{n-1}$ since the size of the conjugacy class of x_1 is at most half the order of the group, and the fact that $x_2, \ldots x_n$ must also commute with each other can only reduce the probability of getting a mutually commuting n-tuple.

Thus we have

$$
\begin{aligned}
Pr_nCom(G) &= Prob(Case1) + Prob(Case2) \\
&< f(1/2)^{n-1}[3-(1/2)^{n-2}] + (1/2)^{n-1} - f(1/2)^{n-1} \\
&= 2f(1/2)^{n-1} + (1/2)^{n-1} - f(1/2)^{2n-3} \\
&< (1/2)^n + (1/2)^{n-1} - (1/2)^{2n-1} \\
&= (1/2)^n[1+2-(1/2)^{n-1} \\
&= (1/2)^n[3-(1/2)^{n-1}]
\end{aligned}
$$

which is what we wanted to show. □

3 Cyclic n-Tuples In A Finite Group

We remarked earlier that another measure of the commutativity of a finite group is the probability that an n-tuple of group elements generates a cyclic subgroup. For convenience of reference, we make the following definition:

DEFINITION: If G is a finite group, an n-tuple, $(x_1, x_2, \ldots, x_n)$ of group elements is called a *cyclic n-tuple* if $< x_1, x_2, \ldots, x_n >$ is a cyclic subgroup of G.

To correspond with the previous section on mutually commuting n-tuples, we use the following notation. For $n \geq 2$:

$Pr_nCyc(G) =$ the probability that the arbitrary n-tuple $(x_1, x_2, \ldots, x_n)$ is a cyclic $n$tuple.

Obviously, a cyclic n-tuple is a mutually commuting n-tuple, but a mutually commuting n-tuple need not be a cyclic n-tuple. It is therefore very interesting that the upper bound for $Pr_nCyc(G)$ for non-cyclic groups is the same as the upper bound for $Pr_nCom(G)$ for non-abelian groups. The goal of this section is to prove that result. To do so we need the following sub-multiplicative property of $Pr_nCyc(G)$:

LEMMA 3: For all groups G, H, and all $n \in \mathbf{N}^{\times}$, $\mathrm{Pr}_n\mathrm{Cyc}(G \times H) \leq \mathrm{Pr}_n\mathrm{Cyc}(G)\mathrm{Pr}_n\mathrm{Cyc}(H)$.

Proof: Let $(g_1, h_1), \ldots, (g_n, h_n) \in (G \times H)$ be such that $\langle (g_1, h_1), \ldots, (g_n, h_n) \rangle$ is cyclic. Then there exists $(g, h) \in G \times H$ and $s_1, \ldots, s_n \in \mathbf{N}$ such that $(g_i, h_i) = (g, h)^{s_i}$ for all $i \leq n$. But then $g_i = g^{s_i}$ for all $i \leq n$, so $\langle g_1, \ldots, g_n \rangle$ is cyclic; similarly $\langle h_1, \ldots, h_n \rangle$ is cyclic. So the number of

n-tuples which generate a cyclic subgroup in $G \times H$ is less than or equal to the number of n-tuples in G which generate a cyclic subgroup times the number of n-tuples in H which generate a cyclic subgroup, and hence $\mathrm{Pr}_n\mathrm{Cyc}(G \times H) \leq \mathrm{Pr}_n\mathrm{Cyc}(G)\mathrm{Pr}_n\mathrm{Cyc}(H)$. □

As we work towards the main result of this section the following shorthand notation will be useful:

Set $P_n := \dfrac{3}{2^n} - \dfrac{1}{2^{2n-1}}$.

Thus P_n is the upper bound for $Pr_nCom(G)$. We now easily get the main result of this section for all non-abelian groups:

OBSERVATION 4: For all non-abelian groups G and all $n \in \mathbf{N}^\times$, $\mathrm{Pr}_n\mathrm{Cyc}(G) \leq P_n$.

Proof: $\mathrm{Pr}_n\mathrm{Cyc}(G) \leq \mathrm{Pr}_n\mathrm{Com}(G) \leq P_n$. □

The abelian groups are more complicated because the results about $Pr_nCom(G)$ do not apply. The key fact is that every non-cyclic abelian group can be written as a product of the form $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m} \times H$, where H is an abelian group. Most of the proof will focus on understanding what happens to the group $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m}$. The result will then follow from an easy application of Lemma 3.

THEOREM 5: For all abelian, noncyclic groups G and all $n \in \mathbf{N}^\times$, $\mathrm{Pr}_n\mathrm{Cyc}(G) \leq P_n$.

Proof: We first prove, by induction on n, that $\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}) \leq P_n$ for all $n \geq 1, k \geq 1$ and primes p. Clearly $\mathrm{Pr}_1\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}) = 1 = P_1$. Now let $n > 1, k \geq 1$, and a prime p be given, and assume that $\mathrm{Pr}_{n-1}\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}) \leq P_{n-1}$. We will give an upper bound on the number of cyclic n-tuples made up of elements of $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}$.

Consider an n-tuple $(x_1, \ldots, x_n)$ in $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}$. If x_1 is of order p^k, then for $(x_1, \ldots, x_n)$ to be a cyclic n-tuple, each of $x_2, \ldots, x_n$ must be in $\langle x_1 \rangle$, since the only cyclic subgroup containing x_1 is $\langle x_1 \rangle$. There are $p^{2k} - p^{2k-2}$ elements of order p^k in $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}$, and then there are p^k choices for each of the $x_2, \ldots, x_n$, so there are $(p^{2k} - p^{2k-2})p^{k(n-1)}$ $n-$tuples in total with

$|x_1| = p^k$.

If x_1 is not of order p^k, then the number of cyclic n-tuples of group elements is certainly bounded above by the number of choices for x_1 times the number of $(n-1)$-tuples which generate a cyclic subgroup. There are p^{2k-2} choices for x_1, and at most $P_{n-1}(p^{2k(n-1)})$ choices for the $(n-1)$-tuple, so there are at most $p^{2k-2}P_{n-1}p^{2k(n-1)}$ cyclic n-tuples with $|x_1| \neq p^k$.

Therefore,

$$\begin{aligned}
\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^k}) &\leq \frac{(p^{2k} - p^{2k-2})p^{k(n-1)} + p^{2k-2}P_{n-1}p^{2k(n-1)}}{p^{2kn}} \\
&= \frac{P_{n-1}}{p^2} + \left(1 - \frac{1}{p^2}\right)\left(\frac{1}{p^k}\right)^{n-1} \\
&\leq \frac{1}{4}P_{n-1} + \frac{3}{4}\left(\frac{1}{2^k}\right)^{n-1} && (1) \\
&\leq \frac{1}{4}P_{n-1} + \frac{3}{4}\left(\frac{1}{2^{n-1}}\right) && (2) \\
&\leq \frac{1}{4}\left(\frac{3}{2^{n-1}} - \frac{1}{2^{2n-3}}\right) + \frac{3}{4}\left(\frac{1}{2^{n-1}}\right) && (3) \\
&= \frac{3}{2^{n+1}} + \frac{3}{2^{n+1}} - \frac{1}{2^{2n-1}} \\
&= \frac{3}{2^n} - \frac{1}{2^{2n-1}} \\
&= P_n.
\end{aligned}$$

Inequality (1) follows because the expression is maximal when p is minimal; i.e. when $p = 2$. Inequality (2) follows since the expression is maximal when k is minimal; i.e. when $k = 1$. Inequality (3) is obtained by simply substituting in the formula for P_n.

Now we proceed to prove, for all primes p and $n \in \mathbf{N}^{\times}$, that if $1 \leq k \leq m$, then $\left(\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m}) \leq P_n\right) \Rightarrow \left(\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}}) \leq P_n\right)$.

Let $n > 1$, a prime p, and $1 \leq k \leq m$ be given, and assume that $\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m}) \leq P_n$. We will again give an upper bound for the number of cyclic n-tuples in $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}}$.

Consider an n-tuple $(x_1, \ldots, x_n)$ in $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}}$. If all of $x_1, \ldots, x_n$ have order less than p^{m+1}, we can embed the n-tuple in a subgroup isomorphic to $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m}$. If we can embed all such n-tuples in the same such subgroup the induction hypothesis will tell as that there are at most $P_n(p^{(k+m)n})$ cyclic n-tuples of this type. This takes some care.

Consider $S = \{(x_1, x_2, \ldots, x_n) \in \mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}} | |x_i| \leq p^m\}$ Let

$$\begin{aligned} x_1 &= (\alpha_1, \beta_1) \\ x_2 &= (\alpha_2, \beta_2) \\ &\vdots \\ x_n &= (\alpha_n, \beta_n) \end{aligned}$$

where $\alpha_i \in \mathbf{Z}_{p^k}$ and $\beta_j \in \mathbf{Z}_{p^{m+1}}$.

Let $H = \bigcup_S \{x_1, x_2, \ldots, x_n\}$. Let A be the projection of H onto the first component and let B be the projection of H onto the second component. Then $H \subseteq < A > \times < B >$. But $< A > \subseteq \mathbf{Z}_{p^k}$ and $< B > \subseteq \mathbf{Z}_{p^{m+1}}$. In particular this means that $< B >$ is cyclic since $\mathbf{Z}_{p^{m+1}}$ is cyclic. But by our hypothesis, $< B >$ has no elements of order p^{m+1}. Therefore it must be that $< B > \cong \mathbf{Z}_{p^j}$ for some $j \leq m$. Now we have all the elements of S embedded in a single subgroup $< A > \times < B >$ of order at most $p^k p^m$. Thus by the induction hypothesis, there are at most $P_n(p^{(k+m)n})$ cyclic n-tuples with all elements of order less than p^{m+1}. Now suppose that $(x_1, x_2, \ldots, x_n)$ is a cyclic n-tuple with x_i such that $|x_i| = p^{m+1}$, but $|x_j| \neq p^{m+1}$ for $j < i$. Then each of the x_j, with $j \neq i$, must be in $\langle x_i \rangle$. There are $p^k(p^{m+1} - p^m)$ choices for x_i, p^m choices for each x_j where $j < i$, and at most p^{m+1} choices for each x_j where $j > i$. Therefore there are at most $p^k(p^{m+1} - p^m)p^{m(i-1)}p^{(m+1)(n-i)}$ cyclic n-tuples of this type. As we let i range from 1 to n, we count a total of

$$\begin{aligned} &\sum_{i=1}^{n} p^k(p^{m+1} - p^m)p^{m(i-1)}p^{(m+1)(n-i)} \\ &= p^k \sum_{i=1}^{n} (p^{m+1} - p^m)(p^{m(n-1)+n-i}) \\ &= p^k \sum_{i=1}^{n} (p^{m+1+m(n-1)+n-i} - p^{m+m(n-1)+n-i}) \\ &= p^k(p^{m+1+m(n-1)+n-1} - p^{m+m(n-1)}) \\ &= p^k(p^{(m+1)n} - p^{mn}) \end{aligned}$$

cyclic n-tuples of this type (that is, cyclic n-tuples with at least one element of order p^{m+1}).

Therefore, combining these two kinds of cyclic n-tuples, we get

$$\mathrm{Pr}_n \mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}}) \leq \frac{P_n(p^{(k+m)n}) + p^k(p^{(m+1)n} - p^{mn})}{p^{(k+m+1)n}}$$

$$
\begin{aligned}
&= \frac{P_n}{p^n} + \frac{p^k(p^{(m+1)n} - p^{mn})}{p^{(k+m+1)n}} \\
&= \frac{P_n}{p^n} + \frac{1}{p^{(n-1)k}} - \frac{1}{p^{(n-1)k+n}} \\
&\leq \frac{P_n}{2^n} + \frac{1}{2^{(n-1)k}} - \frac{1}{2^{(n-1)k+n}} \qquad (4) \\
&\leq \frac{P_n}{2^n} + \frac{1}{2^{n-1}} - \frac{1}{2^{2n-1}} \qquad (5) \\
&= \left(\frac{3}{2^n} - \frac{1}{2^{2n-1}}\right)\frac{1}{2^n} + \frac{1}{2^{n-1}} - \frac{1}{2^{2n-1}} \qquad (6) \\
&= \frac{1}{2^{n-1}} + \frac{3}{2^{2n}} - \left(\frac{1}{2^{2n-1}} + \frac{1}{2^{3n-1}}\right) \\
&\leq \frac{3}{2^n} - \frac{1}{2^{2n-1}} \text{for} n \geq 2 \\
&= P_n.
\end{aligned}
$$

As before, inequality (4) holds since the expression is maximal when p is minimal; i.e. when $p = 2$. Inequality (5) holds since the expression is maximal when k is minimal; i.e. when $k = 1$. Inequality (6) is obtained by substituting in the formula for P_n.

We have now shown that for any group G isomorphic to a group of the form $\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m}, Pr_nCyc(G) \leq P_n$. To complete the proof of our theorem, we note that if G is an abelian non-cyclic group, then $G \cong \mathbf{Z}_{p^k} \times \mathbf{Z}_{p^m} \times H$, where p is prime, $1 \leq k \leq m$, and H is an abelian group. Then applying Lemma 3, we have that

$$
\begin{aligned}
\mathrm{Pr}_n\mathrm{Cyc}(G) &\leq \mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}})\mathrm{Pr}_n\mathrm{Cyc}(H) \\
&\leq \mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_{p^k} \times \mathbf{Z}_{p^{m+1}})\mathrm{since} Pr_nCyc \leq 1 \text{for any group } H \\
&\leq P_n
\end{aligned}
$$

and the proof is complete. □

THEOREM 6: For any non-cyclic finite group, G, $Pr_nCyc(G) \leq P_n$.
Proof: This is merely a combination of Observation 4 and Theorem 5.

We note that the bound in Theorem 6 is sharp, since $\mathrm{Pr}_n\mathrm{Cyc}(\mathbf{Z}_2 \times \mathbf{Z}_2) = P_n$ for all $n \in \mathbf{N}^{\times}$.

4 References

1. P. Erdös and E.G. Strauss, *How abelian is a finite group?* Lin. and Multilin. Alg. 3 (1976) 307-312.

2. J.L. Leavitt, G.J. Sherman and M.E. Walker, *Rewriteability in finite groups*, Amer. Math. Monthly 99 (1992) 446-452.

David Patrick
Carnegie Mellon

Catherine Sugar
Pomona College

Eric Wepsic
Harvard University