WHAT'S THE PROBABILITY OF GENERATING A CYCLIC SUBGROUP?

D. M. Patrick, G. J. Sherman, C. A. Sugar and E. K. Wepsic

1. Introduction

A recent coffee-room conversation at Rose-Hulman about an old number theory gem — two randomly chosen integers are relatively prime with probability $6/\pi^2$ — led to the following exchange.

A group theorist: "You know, $6/\pi^2$ sounds a lot like the 5/8 bound for commutativity to me."

$\mathrm{Pr}_2\mathrm{Comm}(G) = \dfrac{|\{(x,y) \in G^2 \mid xy = yx\}|}{|G|^2}$ is either one or at most 5/8 for finite groups [2].

A topologist: "Oh no! What are you going to do, turn that one into a group theory problem too?"

Here's a try: If x and y are group elements instead of integers, then "are relatively prime" should mean there does not exist an element g in the group such that g "divides" both x and y. Unfortunately (at least for this interpretation) the equations $gz = x$ and $gz = y$ each have solutions for any g in the group. Another try — 6 and 9 are not relatively prime because they generate a proper (cyclic, of course) subgroup of the integers, — suggests the title of this paper.

More formally, let G be a finite group and set

$$\mathrm{Pr}_2\mathrm{Cyc}(G) = \frac{|\{(x,y) \in G^2 \mid \langle x,y\rangle \text{ is cyclic}\}|}{|G|^2}.$$

The work of each of the authors was supported by NSF grant number DMS-910059

If $\langle x,y\rangle$ is cyclic, we say the ordered pair (x,y) is cyclic. The purpose of this note is to show that if G is not cyclic, then $\mathrm{Pr}_2\mathrm{Cyc}(G) \le 5/8$. A generalization to cyclic n-tuples — an n-tuple $(x_1, x_2, \ldots, x_n)$ for which $\langle x_1, x_2, \ldots, x_n\rangle$ is cyclic — is also established.

It is well known that the 5/8 bound for commutativity can be replaced by $(p^2+p-1)/p^3$ where p is the smallest prime dividing the order of G. Rewriting our results in terms of p is left as an exercise for the reader.

2. Cyclic Ordered Pairs

Theorem 1. $\mathrm{Pr}_2\mathrm{Cyc}(G) = 1$ *if G is cyclic; in every other case,* $\mathrm{Pr}_2\mathrm{Cyc}(G) \le 5/8$.

Our proof is woven from the 5/8 bound for commutativity and a sequence of lemmas. Suppose firstly that G is non-abelian. Then, since two elements that generate a cyclic subgroup must commute,

$$\mathrm{Pr}_2\mathrm{Cyc}(G) \le \mathrm{Pr}_2\mathrm{Comm}(G) \le 5/8$$

by the result of [2]. And fortunately,

Lemma 1. $\mathrm{Pr}_2\mathrm{Cyc}(G) = 1$ *if, and only if, G is cyclic.*

Proof: If G is cyclic, certainly each subgroup of G is cyclic; i.e., $\mathrm{Pr}_2\mathrm{Cyc}(G) = 1$. On the other hand, if $\mathrm{Pr}_2\mathrm{Cyc}(G) = 1$, then G is certainly abelian and $\mathrm{Pr}_2\mathrm{Cyc}(S_p) = 1$ for each p-Sylow subgroup of G. This means each p-Sylow subgroup is cyclic and, therefore, that G is cyclic.

Now we may restrict our attention to non-cyclic abelian groups.

Lemma 2. *If $G \cong H \oplus K$, then*

$$\mathrm{Pr}_2\mathrm{Cyc}(G) \le \mathrm{Pr}_2\mathrm{Cyc}(H) \cdot \mathrm{Pr}_2\mathrm{Cyc}(K);$$

i.e., $\mathrm{Pr}_2\mathrm{Cyc}(G)$ *is submultiplicative.*

Proof: If the pair $((x_1,y_1),(x_2,y_2))$ is cyclic, then there exists (x,y) in $H \oplus K$ and there exist non-negative integers s_1 and s_2 such that $(x,y)^{s_i} = (x_i,y_i)$; i.e., both (x_1,x_2) and (y_1,y_2) are cyclic.

In view of Lemma 2,

$$\Pr_2\mathrm{Cyc}(G) \leq \prod_{p||G|} \Pr_2\mathrm{Cyc}(S_p).$$

where p denotes a prime and S_p is the p-Sylow subgroup of G. Thus, if $\Pr_2\mathrm{Cyc}(S_p) \leq 5/8$ for at least one p, the theorem follows.

Since G is non-cyclic, there exists at least one prime, say q, for which S_q is non-cyclic. This means that S_q is of the form $\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^m} \oplus A$ with $1 \leq k \leq m$.

Lemma 3. $\Pr_2\mathrm{Cyc}(\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^k}) \leq 5/8$.

Proof: Let $((a,b),(c,d))$ be a cyclic ordered pair in $\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^k}$. We proceed by cases.

Case: The order of (a,b) is q^k. Since q^k is the maximum order of an element of $\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^k}$, it follows that $(c,d) \in \langle(a,b)\rangle$. Thus there are $q^{2k} - q^{2k-2}$ choices for (a,b) and q^k choices for (c,d); i.e., there are $(q^{2k} - q^{2k-2})q^k$ choices for $((a,b),(c,d))$.

Case: The order of (a,b) is less than q^k. The number of choices for (a,b) is q^{2k-2} and the number of choices for (c,d) is certainly bounded above by q^{2k}; i.e., there are at most $q^{2k-2} \cdot q^{2k}$ choices for $((a,b),(c,d))$.

Therefore,

$$\begin{aligned}\Pr_2\mathrm{Cyc}(\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^k}) &\leq \frac{(q^{2k} - q^{2k-2})q^k + q^{2k-2} \cdot q^{2k}}{q^{4k}} \\ &= \frac{1}{q^2} + \left(1 - \frac{1}{q^2}\right)\left(\frac{1}{q^k}\right) \\ &\leq \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} \\ &= \frac{5}{8}.\end{aligned}$$

It is easy to check that $\Pr_2\mathrm{Cyc}(\mathbf{Z}_2 \oplus \mathbf{Z}_2) = 5/8$.

Lemma 4. $\Pr_2\mathrm{Cyc}(\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^m}) \leq 5/8$ *implies that* $\Pr_2\mathrm{Cyc}(\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^{m+1}}) \leq 5/8$.

Proof: Let $((a,b),(c,d))$ be a cyclic ordered pair in $\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^{m+1}}$. Again, we proceed by cases.

Case: $|(a,b)|, |(c,d)| \leq m$. Let's collect all such cyclic ordered pairs in a set, say $C = \{((a,b),(c,d)) \mid |(a,b)|, |(c,d)| \leq m\}$, and collect the components of elements of C in a set, say $H = \bigcup_C \{(a,b),(c,d)\}$. Now denoting the projection of H onto $\mathbf{Z}_{q^{m+1}}$ by B, we have $H \subseteq \langle A\rangle \oplus \langle B\rangle$. Thus $\langle B\rangle$ is a cyclic subgroup of $\mathbf{Z}_{q^{m+1}}$ containing no elements of order q^{m+1}. Therefore $\langle B\rangle \cong \mathbf{Z}_{q^j}$, where $j \leq m$, which implies that $\langle A\rangle \oplus \langle B\rangle$ is isomorphic to a subgroup of $\mathbf{Z}_{q^n} \oplus \mathbf{Z}_{q^m}$. Our inductive hypothesis yields $|C| \leq (5/8)q^{2(k+m)}$.

Case: $|(a,b)| = q^{m+1}$. There are $q^{k+m+1} - q^{k+m}$ choices for (a,b) and q^{m+1} choices for (c,d) since $(c,d) \in \langle(a,b)\rangle$. Therefore, there are $q^{k+2m+2} - q^{k+2m+1}$ choices for $((a,b),(c,d))$.

Case: $|(a,b)| \leq q^m$ and $|(c,d)| = q^{m+1}$. There are $q^{k+m+1} - q^{k+m}$ choices for (c,d) and q^m choices for (a,b) since $(a,b) \in \langle(c,d)\rangle$ and has order less than q^{m+1}. Therefore, there are $q^{k+2m+1} - q^{k+2m}$ choices for $((a,b),(c,d))$.

Now we have

$$\begin{aligned}\Pr_2\mathrm{Cyc}(\mathbf{Z}_{q^k} \oplus \mathbf{Z}_{q^{m+1}}) &\leq \frac{(5/8)q^{2(k+m)} + q^{k+2m+2} - q^{k+2m}}{q^{2(k+m+1)}} \\ &= \frac{5}{8} \cdot \frac{1}{q^2} + \frac{1}{q^k} - \frac{1}{q^{k+2}} \\ &\leq \frac{5}{8} \cdot \frac{1}{2^2} + \frac{1}{2^k} - \frac{1}{2^{k+2}} \\ &\leq \frac{5}{8} \cdot \frac{1}{2^2} + \frac{1}{2} - \frac{1}{2^3} \\ &= \frac{17}{32}.\end{aligned}$$

Therefore $\Pr_2\mathrm{Cyc}(S_q) \leq 5/8$ and the proof of the theorem is complete.

3. Cyclic n-tuples

Does the theorem generalize to cyclic n-tuples? It hinges on the availability of a 5/8-like bound for $\Pr_n\mathrm{Comm}(G)$, the proportion of mutually commutative n-tuples ($x_ix_j = x_jx_i$ for all i and j) in G. Erdös and Strauss [1] established a lower bound for

$\Pr_n\mathrm{Comm}(G)$ but the following upper bound does not appear to be well-known. Indeed, to the best of our knowledge, this upper bound has appeared only in an unpublished note (Testing Laws in Groups) of John D. Dixon's which circulated in the late 1970's. We include it here with our elementary proof.

Lemma 5. *If G is nonabelian, then*

$$\Pr_n\mathrm{Comm}(G) \leq \frac{3}{2^n} - \frac{1}{2^{2n-1}}.$$

Proof: Given the 5/8 bound for $n = 2$, one observes that either the first component of a mutually commutative n-tuple is in the center, $Z = Z(G)$, of G (with probability $|Z|/|G|$) or it isn't (with probability $1 - |Z|/|G|$). Thus,

$$\begin{aligned}
\Pr_n\mathrm{Comm}(G) &\leq \frac{|Z|}{|G|}\cdot\left(\frac{3}{2^{n-1}} - \frac{1}{2^{2n-3}}\right) + \left(1 - \frac{|Z|}{|G|}\right)\cdot\frac{1}{2^{n-1}} \\
&= \frac{|Z|}{|G|}\cdot\left(\frac{3}{2^{n-1}} - \frac{1}{2^{2n-3}} - \frac{1}{2^{n-1}}\right) + \frac{1}{2^{n-1}} \\
&\leq \frac{1}{4}\left(\frac{3}{2^{n-1}} - \frac{1}{2^{2n-3}} - \frac{1}{2^{n-1}}\right) + \frac{1}{2^{n-1}} \\
&= \frac{3}{2^n} - \frac{1}{2^{2n-1}},
\end{aligned}$$

because $|Z|/|G| \leq 1/4$ and each component must be in the centralizer of the first component. We remark that $\Pr_n\mathrm{Comm}(G)$ assumes the bound if, and only if, $G/Z \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$.

With Lemma 5 in hand one can generalize the proof of the Theorem 1 to cyclic n-tuples by replacing each occurrence of 5/8 with $\frac{3}{2^n} - \frac{1}{2^{2n-1}}$:

Theorem 2. $\Pr_n\mathrm{Cyc}(G)$ *is either one or it is at most* $\frac{3}{2^n} - \frac{1}{2^{2n-1}}$.

Acknowledgement.

Group-theoretic experimentation was facilitated by the computer algebra system CAYLEY.

References

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

[2] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

D. M. Patrick,
Department of Mathematics,
Massachusetts Institute of Technology,
Cambridge, MA 02139,
USA.

G. J. Sherman,
Department of Mathematics,
Rose-Hulman Institute of Technology,
Terre Haute, IN 47803,
USA.

C. A. Sugar,
Department of Mathematics,
Stanford University,
Stanford, CA 94305,
USA.

E. K. Wepsic,
Department of Mathematics,
Harvard University,
Cambridge, MA 02138,
USA.