A left coset composed of n-cycles

Don Coppersmith*

September 18, 2001

Abstract

Let S_n be the symmetric group on n elements. Let $g = (1, 2, \ldots, n) \in S_n$ be an n-cycle. Suppose that $H \subseteq S_n$ is a permutation group. We say that H *has property* P *with respect to* g *and* S_n, or H *has* $P(g, S_n)$, if, for each permutation $h \in H$, the product gh is an n-cycle.

The purpose of this note is to give an upper bound on the size of any group H having property $P(g, S_n)$.

This is a revised version of IBM Research Report 19511 dated April 1994.

1 Notation

Let S_n be the symmetric group on n elements. Let $g = (1, 2, \ldots, n) \in S_n$ be an n-cycle. Suppose that $H \subseteq S_n$ is a permutation group. We say that H *has property* P *with respect to* g *and* S_n, or H *has* $P(g, S_n)$, if, for each permutation $h \in H$, the product gh is an n-cycle.

A permutation group $H \subseteq S_n$ defines a *partition* of $\{1, 2, \ldots, n\}$ into *blocks* $B_i \subseteq \{1, 2, \ldots, n\}$, such that for any two members $x, y \in B_i$ there is a group element $h \in H$ with $h(x) = y$, while if $x \in B_i, y \in B_j, i \neq j$ there is no such group element $h \in H$ with $h(x) = y$.

The *stabilizer* of a subset $X \subseteq \{1, 2, \ldots, n\}$ is defined as

$$H_X = \{h \in H | \forall x \in X, h(x) = x\},$$

*IBM T.J. Watson Research Center, Yorktown Heights, NY, 10598

the set of permutations $h \in H$ fixing each element of X. If X is a singleton $X = \{k\}$, we write $H_k = H_{\{k\}}$.

Lemma 1 *Suppose H has property $P(g, S_n)$. Then no block B_i of H contains two adjacent elements $\{k, k+1\}$. (We consider $n, 1$ to be adjacent.)*

Proof : Assume the contrary: $k, k+1 \in B_i$. Then there is a permutation $h \in H$ with $h(k+1) = k$. The product gh has a fixed point: $g(h(k+1)) = k+1$, contradicting property P. $\square$

Corollary 1 *No block has size exceeding $n/2$.*

Lemma 2 *Suppose H has property $P(g, S_n)$. Then the stabilizer H_k, viewed as a subgroup of the symmetric group on $\{1, 2, \ldots, k-1, k+1, \ldots, n\}$, has property P with respect to $g' = (1, 2, \ldots, k-1, k+1, \ldots, n)$ and $S_{n-1} = S_{\{1,2,\ldots,k-1,k+1,\ldots,n\}}$.*

Proof : Consider a permutation $h' \in H_k \subseteq S_n - 1$, and h, the corresponding member of $H \subseteq S_n$. Set $j = h^{-1}(k-1)$. The n-cycle $gh \in S_n$ satisfies $g(h(j)) = k$, $g(h(k)) = k+1$. The permutation $g'h' \in S_{n-1}$ differs from gh in that $g'(h'(j)) = g'(k-1) = k+1$, while for all $i \neq j, k$ we have $g'(h'(i)) = g(h(i))$. So $g'h'$ is the $(n-1)$-cycle obtained by deleting k from the n-cycle gh. $\square$

Lemma 3 *Suppose H is a permutation group and B_i are the blocks of H. Each block of H_k is contained in some block B_i of H. (The partition induced by H_k is a refinement of the partition induced by H, except that k is not in any block ${B'}_i$ of H_k.)*

Proof : Standard permutation group theory. $\square$

Lemma 4 *Suppose H is a permutation group, B_i is a block of H, and $k \in B_i$. Then*

$$|H| = |B_i| * |H_k|.$$

Proof : Standard permutation group theory. $\square$

Lemma 5 *For any ϵ with $0 < \epsilon < 1/2$, set $\alpha = 1/2 + \epsilon$, $\beta = \epsilon$. Let n be sufficiently large: larger than some N_ϵ depending only on ϵ. Let the parameters $f, \delta, |D|, |Y|, |Z|$ satisfy*

$$\begin{gathered} 1 \leq f \leq \min\{n^{\alpha/(1-\beta)}, |D|/2\} \\ \sqrt{n}\log n \leq |D| \leq n \\ \delta \leq |D| \\ 0 \leq |Y| \leq \tfrac{n}{|D|} - 1 \\ 0 \leq |Z| \leq \tfrac{|D|}{f}(\log f + 1) \end{gathered}$$

Then we have

$$\begin{gathered} [(|Y| + |Z|)\log\delta + |D|\log f] - \alpha(|Y| + |Z| + |D|)\log n - \\ -\beta\,[(|Y| + |Z|)\log\delta + |D|\log|D|] \leq 0. \end{gathered}$$

Proof : Since $\delta \leq |D|$ and $\beta < 1$, we can replace δ by $|D|$ throughout. We consider two cases for the value of f.

Case 1. Suppose $1 \leq f \leq 1/\epsilon^2$. Then from

$$|Y| + |Z| \leq |D|\left(1 + \frac{1}{\log^2 n}\right) \leq |D|\left(1 + \frac{\epsilon}{2}\right)$$

$$\log f \leq \frac{\epsilon}{2}\log n$$

(for n large enough), we get

$$(|Y| + |Z|)\log\delta + |D|\log f \leq (|Y| + |Z| + |D|)(\log n)(\frac{1}{2} + \epsilon).$$

Case 2. Suppose $1/\epsilon^2 \leq f \leq |D|/2$. Then $|Y| + |Z| \leq \epsilon|D|$. The target expression is bounded by

$$(|Y|+|Z|+|D|)(\log f - \alpha\log n - \beta\log f) + ((|Y|+|Z|)(1-\beta) - \beta|D|)(\log|D|/f).$$

The upper bound on f forces $(\log f - \alpha\log n - \beta\log f) \leq 0$, making the first term negative, and $|Y| + |Z| \leq \epsilon|D|$ makes the second term negative. □

Lemma 6 *Let α, β, n be as before. Let the parameters $f, \delta, |D|, |Y|, |Z|$ satisfy*

$$\begin{gathered} n^{\alpha/(1-\beta)} \leq f \leq |D|/2 \\ \sqrt{n} \log n \leq |D| \leq n \\ \delta \leq |D| \\ 0 \leq |Y| \leq \tfrac{n}{|D|} - 1 \\ 0 \leq |Z| \leq \tfrac{|D|}{f}(\log f + 1). \end{gathered}$$

(The condition on f has changed.) Then we have

$$(|Y|+|Z|)\log\delta - \alpha(|Y|+|Z|)\log n - \beta\left[(|Y|+|Z|)\log\delta + |D|\log\{|D|/f\}\right] \leq 0.$$

Proof : Again we can set $\delta = |D|$. We have

$$|Y| + |Z| \leq |D|\left(\frac{1}{\log^2 n} + n^{-3\epsilon/2}\right) \leq \frac{2|D|}{\log^2 n}$$

so that

$$\begin{aligned} &(|Y| + |Z|)\log\delta - \alpha(|Y| + |Z|)\log n - \beta(|Y| + |Z|)\log\delta \\ &\leq \tfrac{2|D|}{\log^2 n}((1-\beta)\log|D| - \alpha\log n) \\ &\leq \tfrac{2|D|}{\log^2 n}\left(\tfrac{\log n}{2}\right) \leq \tfrac{|D|}{\log n}, \end{aligned}$$

while

$$-\beta|D|\log\{|D|/f\} \leq -\beta|D|\log 2,$$

so that as long as n is big enough ($n > \exp[1/(\epsilon\log 2)]$) the desired inequality holds. □

Lemma 7 *Let α, β, n be as before, and set $\gamma = \log(N_\epsilon!)$. Suppose H is a permutation group, B_i are the blocks of H, and $b_i = |B_i|$ Then we have*

$$\log|H| \leq \alpha n\log n + \beta\sum b_i\log b_i + \gamma.$$

Proof : Let D be the largest block of H with $d = |D|$. If $d < \sqrt{n}\log n$, or if $n \leq N_\epsilon$, then the proof is immediate.

Suppose $d \geq \sqrt{n}\log n$ and $n > N_\epsilon$. Consider two elements of D closest together in the cyclic order. They are separated by at most $(n/d - 1) \leq \sqrt{n}/\log n$ elements of $\{1, 2, \ldots, n\} - D$. Let X denote the set of these separating elements. Consider their stabilizer H_X. Since the removal of X brings two elements of D into adjacent positions, the block D is broken into at least two pieces in this stabilizer.

In $H = H_\phi$ (stabilizing on the empty set) D is not broken, while in H_X we have that D is broken. So there is some subset $Y \subseteq X$ and an element $x \in X - Y$ so that D is intact in H_Y but broken in $H_{Y\cup\{x\}}$. Let E be the block containing x in the partition induced by H_Y.

Let f be the size of the smallest subblock of D in the partition induced by $H_{Y\cup\{x\}}$. We claim that we can find a subset $Z \subseteq E$ of size $|Z| = z \leq (d/f)(\log f + 1)$ such that, in $H_{Y\cup Z}$, D is completely broken into subblocks of size at most f. The reason is that H_Y acts transitively on D. Let $J \subseteq D$ be a subblock of size f in the partition induced by $H_{Y\cup\{x\}} = (H_Y)_x$. For each $h \in H_Y$, the conjugate of $(H_Y)_x$ by h is the stabilizer of $x' = h(x)$, namely $(H_Y)_{x'}$. This conjugation also maps J to some subblock $J' \subseteq D$ of size f. Further, Y, Z, D are all disjoint. Build an $|H_Y| \times |D|$ matrix, with rows indexed by $h \in H_Y$ and columns by $j \in D$, whose (h, j) entry is 1 if $j \in J'$ is in the conjugate of J by h. The matrix has constant row sum f and constant column sum $f|H_Y|/|D|$. By a greedy algorithm we can select at most $(d/f)(\log f + 1)$ rows which cover all the columns[1]. For each selected row h, put $x' = h(x)$ into the set Z. For each $j \in D$, there is some selected row h and thus some $x' \in Z$ so that $(H_Y)_{x'}$ induces a partition in which j is in a block of size f. Then $(H_Y)_Z = H_{Y\cup Z}$ induces a partition in which all of D is broken into blocks of size at most f.

Now break into cases depending on the size of f.

Case 1. If $\log f \leq (\alpha \log n)/(1 - \beta)$, then we consider the stabilizer $H_{Y\cup Z\cup D}$. We first estimate $|H|/|H_{Y\cup Z\cup D}|$. Considering the effect of stabilizing on elements first of Y, then of Z, then of D, we find the following upper bound on this ratio:

$$\log\left(|H|/|H_{Y\cup Z\cup D}|\right) \leq (|Y| + |Z|)\log|D| + |D|\log f.$$

This follows because each element of $Y \cup Z$ was originally in a block of size at most $|D|$. We will need a more delicate estimate. We define $\delta \leq |D|$ by

$$(|Y| + |Z|)\log\delta = \sum_{y\in Y\cup Z}\log b_y,$$

[1] Probably better off to cover half the columns in (d/f) rows and eliminate the $(\log f)$ factor.

where b_y is the size of the block containing y in the partition induced by H. Then we have

$$\log\left(|H|/|H_{Y\cup Z\cup D}|\right) \leq (|Y|+|Z|)\log\delta + |D|\log f.$$

Say the group $H_{Y\cup Z\cup D}$ breaks $\{1,2,\ldots,n\}-(Y\cup Z\cup D)$ into blocks of size ${b'}_i$, with

$$n' = \sum {b'}_i = n - |Y\cup Z\cup D|.$$

We have, by induction,

$$\log|H_{Y\cup Z\cup D}| \leq \alpha n'\log n' + \beta\sum {b'}_i\log {b'}_i \leq \alpha n'\log n + \beta\sum {b'}_i\log {b'}_i + \gamma.$$

Further, we have

$$\alpha n\log n - \alpha n'\log n = \alpha(n-n')\log n = \alpha(|Y|+|Z|+|D|)\log n$$

and

$$\beta\sum b_i\log b_i - \beta\sum {b'}_i\log {b'}_i \geq \beta\left[(|Y|+|Z|)\log\delta + |D|\log|D|\right].$$

Combining,

$$\begin{array}{rcl}\log|H| & \leq & [(|Y|+|Z|)\log\delta + |D|\log f] + \alpha n'\log n + \beta\sum {b'}_i\log {b'}_i + \gamma \\ & \leq & [(|Y|+|Z|)\log\delta + |D|\log f] + \alpha n\log n + \beta\sum b_i\log b_i - \\ & & -\alpha(|Y|+|Z|+|D|)\log n - \beta\left[(|Y|+|Z|)\log\delta + |D|\log|D|\right] + \gamma\end{array}$$

Applying Lemma 5, we obtain

$$\log|H| \leq \alpha n\log n + \beta\sum b_i\log b_i + \gamma,$$

as desired.

Case 2. If $(\alpha\log n)/(1-\beta) \leq f \leq |D|/2$, then we consider the stabilizer $H_{Y\cup Z}$. We define δ as before:

$$(|Y|+|Z|)\log\delta = \sum_{y\in Y\cup Z}\log b_y$$

where b_y is the size of the block containing Y in the partition induced by H. Then we estimate

$$\log\left(|H|/|H_{Y\cup Z}|\right) \leq (|Y|+|Z|)\log\delta.$$

As before, the group $H_{Y \cup Z}$ breaks $\{1, 2, \ldots, n\} - (Y \cup Z)$ into blocks of size ${b'}_i$, with

$$n' = \sum {b'}_i = n - |Y \cup Z|.$$

We have, by induction,

$$\log |H_{Y \cup Z}| \leq \alpha n' \log n + \beta \sum {b'}_i \log {b'}_i + \gamma.$$

Further, we have

$$\alpha n \log n - \alpha n' \log n = \alpha(|Y| + |Z|) \log n$$

and

$$\beta \sum b_i \log b_i - \beta \sum {b'}_i \log {b'}_i \geq \beta \left[(|Y| + |Z|) \log \delta + |D| \log\{|D|/f\} \right].$$

Combining,

$$\begin{aligned} \log |H| &\leq (|Y| + |Z|) \log \delta + \alpha n' \log n + \beta \textstyle\sum {b'}_i \log {b'}_i + \gamma \\ &\leq (|Y| + |Z|) \log \delta + \alpha n \log n + \beta \textstyle\sum b_i \log b_i - \\ &\quad -\alpha(|Y| + |Z|) \log n - \beta \left[(|Y| + |Z|) \log \delta + |D| \log\{|D|/f\} \right] + \gamma. \end{aligned}$$

Apply Lemma 6 to obtain

$$\log |H| \leq \alpha n \log n + \beta \sum b_i \log b_i + \gamma,$$

as desired. □

Theorem 1

$$|H| \leq n^{(1/2 + o(1))n}.$$

Proof : Lemma 7, together with the estimates $\alpha = 1/2 + \epsilon, \beta = \epsilon$, and letting $\epsilon \to 0$ sufficiently slowly that γ remains $o(n \log n)$. □

2 Extensions

To prove better upper bounds, we will need different proof techniques. We have been relying only on blocks of transitivity, the fact that no such block contains two adjacent elements, and the properties of stabilizers.

Let n be even, and consider the following set H of permutations on $\{1, 2, \ldots, n\}$. (Note: H is not a group.) H is the set of permutations g mapping even integers to even integers and odd to odd, such that for any odd integer $k, 1 \leq k < n$, $g(g(k)+1) = k+1$. The action of g on the odd integers is free, and determines its action on the even integers, so that $|H| = (n/2)! = (n!)^{1/2+o(1)}$. The blocks of transitivity behave correctly, as do the stabilizers. For each $g \in H$, the product g' of g with the permutation $(1, 2, \ldots, n)$ is an n-cycle, since for k odd we have $g'(g'(k)) = k+2$. Any power of an element of H is contained in H.

But H is not a group; the elements compose badly. Let $g_1, g_2 \in H$, and k be odd. Suppose $g_1(k) = \ell$, and $g_2(\ell) = m$. Then $g_2(m+1) = \ell+1$, and $g_1(\ell+1) = k+1$. But to compose these into a permutation g_3 with $g_3(k) = m, g_3(m+1) = k+1$, requires $g_2 \circ g_1$ on odd elements and $g_1 \circ g_2$ on even elements.

Since H is not a group, it is not a candidate for our study; but it satisfies the rest of our lemmas. So stronger techniques will be needed to outlaw such sets, and to get improved upper bounds.

3 Lower bounds

When n is a power of 2, we can get a lower bound of $2^n/(2n)$. The example is a group of automorphisms of a binary tree with n nodes, consisting of an even number of transpositions at each level of the tree.

Number the elements $0, 1, \ldots, n-1$, where $n = 2^k$. We will define a group H by describing a typical element. For each integer $i = 1, 2, \ldots, n-1$, select a subset $X_i \subseteq \{0, 1, \ldots, 2^i - 1\}$ with even cardinality. Define the permutation h_{i,X_i} by

$$h_{i,X_i}(m) = \begin{cases} m + 2^i & \text{if} \quad (m \bmod 2^{i+1}) \in X_i \\ m - 2^i & \text{if} \quad ((m \bmod 2^{i+1}) - 2^i) \in X_i \\ m & \text{otherwise} \end{cases}$$

When X_i is understood, we will write simply h_i. A typical element of H is the product of permutations h_{i,H_i}:

$$h = h_{k-1,X_{k-1}} h_{k-2,X_{k-2}} \ldots h_{2,X_2} h_{1,X_1}.$$

For completeness we could add h_{0,X_0}, but the only subset X_0 of $\{0\}$ of even cardinality is the empty set, so that h_{0,X_0} is the identity permutation.

We need to show that H defines a group. It helps to notice that, if $i < j$, we have

$$h_{i,X_i} h_{j,X_j} = h_{j,X'_j} h_{i,X_i},$$

where

$$X'_j = h_{i,X_i}(X_j).$$

Details are left to the reader.

To show that H enjoys property P, let $h = h_{k-1,X_{k-1}} \dots h_{2,X_2} h_{1,X_1}$ and consider the cycle c of gh containing the element 0. Because gh takes even numbers to odd numbers and odd to even, the cycle must be balanced in the sense that half its elements are odd and half are even.

Select $j \in \{1, 2, \dots, k-1\}$. The behavior of $gh \bmod 2^j$ is determined by the sets $X_1, \dots, X_{j-1}$. Suppose that the cycle is evenly distributed $\mathrm{mod} 2^j$. Then, viewed $\bmod 2^j$, the cycle looks like $|c|/2^j$ iterations of a cycle of length 2^j. After one such iteration, each residue class $\mathrm{mod} 2^j$ has been hit exactly once. Also, for each for residue class $m \bmod 2^{j+1}$ with $0 \le m \le 2^j - 1$, either m or $m + 2^j$ has been hit exactly once mod ${}^{j+1}$. That means that in the permutation h_{j,X_j} each transposition due to an element of X_j has occurred exactly once. If $(p \bmod 2^{j+1}) = m$, and if $m \in X_j$ or $m - 2^j \in X_j$, then $h_j(p) \equiv p + 2^j (\mathrm{mod} 2^{j+1})$. Otherwise $h_j(p) \equiv p (\mathrm{mod} 2^{j+1})$. For $i > j$, $h_i(p) \equiv p \bmod (2j+1)$. For $i < j$, since the cycle is balanced mod 2^j, the number of increases by 2^i due to h_i is equal to the number of decreases by 2^i due to h_i over the course of 2^j steps. Finally, each application of g adds 1 to the value. Since $|X_j|$ is even, we see that in the course of 2^j steps we reach

$$(gh)^{2^j}(p) \equiv p + 2^j + |X| 2^j \equiv p + 2^j (\mathrm{mod} 2^{j+1}).$$

This tells us that in 2^{j+1} steps we execute a full cycle $\mathrm{mod} 2^{j+1}$, and that c is balanced mod 2^{j+1}. By induction, c is balanced mod $n = 2^k$, and c is an n-cycle.

The number of choices for X_i is

$$2^{2^i - 1},$$

the "-1" coming from the requirement that $|X_i|$ be even. So the size of $|H|$

is

$$\begin{aligned}
&2^{(2^0-1)} \times 2^{(2^1-1)} \times 2^{(2^2-1)} \times \cdots \times 2^{(2^{k-1}-1)} \\
&= 2^{\left(2^0+2^1+2^2+\ldots+2^{k-1}-(1+1+\ldots+1)\right)} \\
&= 2^{(2^k-1-k)} = 2^n/(2n).
\end{aligned}$$

If n is not a power of 2, a similar argument shows a weaker lower bound of $f(n) \geq 2^n/n^2$.

4 Summary

We have given bounds on $f(n)$, the size of the largest possible subgroup of S_n with a left coset all of whose elements are n-cycles, namely

$$2^n/n^2 \leq f(n) \leq (n!)^{1/2+o(1)}.$$

A substantial gap remains.

5 Acknowledgement

I thank Thomas Schwentick, then of Universität Mainz, now of Friedrich-Schiller-Universität Jena, for introducing me to this problem.