Permutations contained in transitive groups

Dimitris Koukoulopoulos[1]

Joint work with Sean Eberhard[2] and Kevin Ford[3]

[1]Université de Montréal
[2] University of Oxford
[3] University of Illinois at Urbana-Champaign

15th Panhellenic Conference of Mathematical Analysis,
University of Crete, 28 May 2016

Basic set-up

S_n = set of permutations of $\{1, \ldots, n\}$.

Motivation : understand the subgroup structure of S_n.

Basic set-up

S_n = set of permutations of $\{1, \ldots, n\}$.

Motivation : understand the subgroup structure of S_n.

If $G \leq S_n$, then G acts on $[n] = \{1, \ldots, n\}$.

- G is called transitive if all orbits are the full set $[n]$;
- G is called imprimitive if it permutes a non-trivial partition $(B_1, \ldots, B_\nu)$ of $[n]$;
- if G is transitive and imprimitive, then $|B_i| = |B_j|$ for all i, j.

Basic set-up

S_n = set of permutations of $\{1, \ldots, n\}$.

Motivation : understand the subgroup structure of S_n.

If $G \leq S_n$, then G acts on $[n] = \{1, \ldots, n\}$.

- G is called transitive if all orbits are the full set $[n]$;
- G is called imprimitive if it permutes a non-trivial partition $(B_1, \ldots, B_\nu)$ of $[n]$;
- if G is transitive and imprimitive, then $|B_i| = |B_j|$ for all i, j.

Question

If σ is chosen uniformly at random from S_n, what is the probability that it lies inside a transitive group $G \neq A_n, S_n$?

Basic set-up

S_n = set of permutations of $\{1, \ldots, n\}$.

Motivation : understand the subgroup structure of S_n.

If $G \leq S_n$, then G acts on $[n] = \{1, \ldots, n\}$.

- G is called transitive if all orbits are the full set $[n]$;
- G is called imprimitive if it permutes a non-trivial partition $(B_1, \ldots, B_\nu)$ of $[n]$;
- if G is transitive and imprimitive, then $|B_i| = |B_j|$ for all i, j.

Question

If σ is chosen uniformly at random from S_n, what is the probability that it lies inside a transitive group $G \neq A_n, S_n$?

Question (special case)

If σ is chosen uniformly at random from S_{2n}, what is the probability that it has a fixed subset of size n?

Basic set-up

S_n = set of permutations of $\{1, \dots, n\}$.

Motivation : understand the subgroup structure of S_n.

If $G \leq S_n$, then G acts on $[n] = \{1, \dots, n\}$.

- G is called transitive if all orbits are the full set $[n]$;
- G is called imprimitive if it permutes a non-trivial partition $(B_1, \dots, B_\nu)$ of $[n]$;
- if G is transitive and imprimitive, then $|B_i| = |B_j|$ for all i, j.

Question

If σ is chosen uniformly at random from S_n, what is the probability that it lies inside a transitive group $G \neq A_n, S_n$?

Question (special case)

If σ is chosen uniformly at random from S_{2n}, what is the probability that it has a fixed subset of size n?

Luczak-Pyber (1993): probability is $O(n^{-c})$ for both questions.

Imprimitive transitive subgroups

- G is imprimitive transitive if-f it permutes a partition $(B_1, \ldots, B_\nu)$ of $[n]$ into blocks of equal size n/ν. Here, $1 < \nu < n$ and $\nu | n$.

Imprimitive transitive subgroups

- G is imprimitive transitive if-f it permutes a partition $(B_1, \dots, B_\nu)$ of $[n]$ into blocks of equal size n/ν. Here, $1 < \nu < n$ and $\nu | n$.
- If $\sigma \in S_n$ permutes a partition $(B_1, \dots, B_\nu)$ as above, then let $\tilde{\sigma} \in S_\nu$ be the induced permutation of the blocks $B_1, \dots, B_\nu$, and write $(d_1, \dots, d_\nu)$ for the cycle lengths of $\tilde{\sigma}$.

Imprimitive transitive subgroups

- G is imprimitive transitive if-f it permutes a partition $(B_1, \ldots, B_\nu)$ of $[n]$ into blocks of equal size n/ν. Here, $1 < \nu < n$ and $\nu | n$.
- If $\sigma \in S_n$ permutes a partition $(B_1, \ldots, B_\nu)$ as above, then let $\tilde{\sigma} \in S_\nu$ be the induced permutation of the blocks $B_1, \ldots, B_\nu$, and write $(d_1, \ldots, d_\nu)$ for the cycle lengths of $\tilde{\sigma}$.
- Then σ fixes each set of a partition $(C_1, \ldots, C_r)$ of $[n]$ with $|C_i| = d_i n/\nu$ and all cycles lengths of $\sigma\big|_{C_i}$ divisible by d_i.

Permutations with fixed subsets of a given size

$$i(n,k) := \mathbb{P}_{\sigma \in S_n}(\sigma \text{ fixes some set of size } k).$$

Permutations with fixed subsets of a given size

$$i(n,k) := \mathbb{P}_{\sigma \in S_n}(\sigma \text{ fixes some set of size } k).$$

$\sigma = \pi_1 \cdots \pi_r$ cycle decomposition, $c_j(\sigma) = \#\{i : |\pi_i| = j\}$

Permutations with fixed subsets of a given size

$$i(n,k) := \mathbb{P}_{\sigma \in S_n}(\sigma \text{ fixes some set of size } k).$$

$\sigma = \pi_1 \cdots \pi_r$ cycle decomposition, $c_j(\sigma) = \#\{i : |\pi_i| = j\}$

$$\mathcal{L}(\sigma) := \{\text{lengths of fixed sets of } \sigma\} = \left\{ \sum_{i \in I} |\pi_i| : I \subset [r] \right\}$$
$$= \left\{ \sum_{j=1}^{n} j b_j \ : \ 0 \le b_j \le c_j(\sigma)\ \forall j \right\}.$$

Permutations with fixed subsets of a given size

$$i(n,k) := \mathbb{P}_{\sigma\in S_n}(\sigma \text{ fixes some set of size } k).$$

$\sigma = \pi_1 \cdots \pi_r$ cycle decomposition, $c_j(\sigma) = \#\{i : |\pi_i| = j\}$

$$\mathcal{L}(\sigma) := \{\text{lengths of fixed sets of } \sigma\} = \left\{ \sum_{i\in I} |\pi_i| : I \subset [r] \right\}$$
$$= \left\{ \sum_{j=1}^{n} j b_j \ : \ 0 \le b_j \le c_j(\sigma)\ \forall j \right\}.$$

$$\mathbb{P}_{\sigma\in S_n}(c_j(\sigma) = m_j \ (1 \le j \le J)) \sim \prod_{j=1}^{J} \frac{e^{-1/j}}{j^{m_j} m_j!}.$$

i.e. the functions $c_j(\sigma)$, $j \le J$, are approximately independent and Poisson of parameters $1/j$, $j \le J$.

Random integers vs. random permutations

$\omega(n; y, z) := \#\{p|n : y < p \le z\}$, $y_0 = e < y_1 < y_2 < \cdots < y_J \le x$

Random integers vs. random permutations

$\omega(n; y, z) := \#\{p | n : y < p \leq z\}$, $y_0 = e < y_1 < y_2 < \cdots < y_J \leq x$

$$\frac{\#\{n \leq x : \omega(n; y_{j-1}, y_j) = m_j \ (j \leq J)\}}{x} \approx \prod_{j=1}^{J} \frac{\log y_{j-1}}{\log y_j} \frac{(\log \frac{\log y_j}{\log y_{j-1}})^{m_j - 1}}{(m_j - 1)!}$$

Random integers vs. random permutations

$\omega(n; y, z) := \#\{p|n : y < p \le z\}$, $y_0 = e < y_1 < y_2 < \cdots < y_J \le x$

$$\frac{\#\{n \le x : \omega(n; y_{j-1}, y_j) = m_j \ (j \le J)\}}{x} \approx \prod_{j=1}^{J} \frac{\log y_{j-1}}{\log y_j} \frac{(\log \frac{\log y_j}{\log y_{j-1}})^{m_j - 1}}{(m_j - 1)!}$$

Also, if $n = p_1 \cdots p_r$ square-free and $\omega_j(n) := \omega(n; e^{j-1}, e^j)$, then

$$\{\log d : d|n\} = \left\{ \sum_{i \in I} \log p_i : I \subset [r] \right\} \text{ `} = \text{' } \left\{ \sum_j j\omega_j(n) \right\}$$

Random integers vs. random permutations

$\omega(n; y, z) := \#\{p|n : y < p \le z\}$, $y_0 = e < y_1 < y_2 < \cdots < y_J \le x$

$$\frac{\#\{n \le x : \omega(n; y_{j-1}, y_j) = m_j \ (j \le J)\}}{x} \approx \prod_{j=1}^{J} \frac{\log y_{j-1}}{\log y_j} \frac{(\log \frac{\log y_j}{\log y_{j-1}})^{m_j - 1}}{(m_j - 1)!}$$

Also, if $n = p_1 \cdots p_r$ square-free and $\omega_j(n) := \omega(n; e^{j-1}, e^j)$, then

$$\{\log d : d|n\} = \left\{ \sum_{i \in I} \log p_i : I \subset [r] \right\} `=` \left\{ \sum_j j\omega_j(n) \right\}$$

Theorem (Ford (2008, $m = 2$) and K. (2010, $m \ge 3$))

Fix $m \ge 2$. For $z_m \ge \cdots \ge z_1 \ge 2$ and $z_{m-1} \le z_1^{O(1)}$,

$$\frac{\#\{n = d_1 \cdots d_m : z_i < d_i \le 2z_i \ \forall i\}}{z_1 \cdots z_m} \asymp \frac{1}{(\log z_1)^{\delta_m} (\log \log z_1)^{3/2}}$$

with $\delta_m = \lambda_m \log \lambda_m - \lambda_m + 1$, $\lambda_m = (m-1)/\log m$.

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma \in S_n}(\sigma \text{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \leq k \leq n/2)$.

Heuristics : take n even, $k = n/2$.

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma \in S_n}(\sigma \textit{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \leq k \leq n/2)$.

Heuristics : take n even, $k = n/2$.

- $\sigma = \pi_1 \cdots \pi_r$; $\quad \#\{I \subset [r] : \sum_{i \in I} |\pi_i| = k\} \approx 2^r/n$;

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma \in S_n}(\sigma \textit{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \leq k \leq n/2)$.

Heuristics : take n even, $k = n/2$.

- $\sigma = \pi_1 \cdots \pi_r$; $\quad \#\{I \subset [r] : \sum_{i \in I} |\pi_i| = k\} \approx 2^r/n$;
- need $2^r/n > 1 \;\Leftrightarrow\; r > \log n / \log 2$;

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma \in S_n}(\sigma \textit{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \le k \le n/2)$.

Heuristics : take n even, $k = n/2$.

- $\sigma = \pi_1 \cdots \pi_r$; $\quad \#\{I \subset [r] : \sum_{i \in I} |\pi_i| = k\} \approx 2^r/n$;
- need $2^r/n > 1 \;\Leftrightarrow\; r > \log n / \log 2$;
- r Poisson of mean $\sum_{j \le n} 1/j \sim \log n$. So $i(n,k) \approx n^{-\delta_1}/\sqrt{\log n}$.

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma\in S_n}(\sigma \textit{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \le k \le n/2)$.

Heuristics : take n even, $k = n/2$.

- $\sigma = \pi_1 \cdots \pi_r$; $\#\{I \subset [r] : \sum_{i\in I} |\pi_i| = k\} \approx 2^r/n$;
- need $2^r/n > 1 \;\Leftrightarrow\; r > \log n/\log 2$;
- r Poisson of mean $\sum_{j\le n} 1/j \sim \log n$. So $i(n,k) \approx n^{-\delta_1}/\sqrt{\log n}$.

Correction: $c_j(\sigma) = \#\{i : |\pi_i| = j\}$ Poisson of parameter $1/j$.

- conditioning to have $r = \log n + O(1)$ cycles,
  $\mathbb{E}[\sum_{j\le e^u} c_j(\sigma)] = r\frac{\sum_{j\le e^u} 1/j}{\sum_{j\le n} 1/j} \sim u/\log 2$.

Transference to the permutation setting

Theorem (Eberhard, Ford, Green (2015))

$i(n,k) = \mathbb{P}_{\sigma \in S_n}(\sigma \textit{ fixes some set of size } k) \asymp \frac{k^{-\delta_1}}{(\log k)^{3/2}}$ $(2 \leq k \leq n/2)$.

Heuristics : take n even, $k = n/2$.

- $\sigma = \pi_1 \cdots \pi_r$; $\quad \#\{I \subset [r] : \sum_{i \in I} |\pi_i| = k\} \approx 2^r/n$;
- need $2^r/n > 1 \;\Leftrightarrow\; r > \log n / \log 2$;
- r Poisson of mean $\sum_{j \leq n} 1/j \sim \log n$. So $i(n,k) \approx n^{-\delta_1}/\sqrt{\log n}$.

Correction: $c_j(\sigma) = \#\{i : |\pi_i| = j\}$ Poisson of parameter $1/j$.

- conditioning to have $r = \log n + O(1)$ cycles, $\mathbb{E}[\sum_{j \leq e^u} c_j(\sigma)] = r \frac{\sum_{j \leq e^u} 1/j}{\sum_{j \leq n} 1/j} \sim u/\log 2$.
- **Ford:** actually, we must have that $\sum_{j \leq e^u} c_j(\sigma) \leq u/\log 2 + O(1)$. Leads to a random walk with a barrier. Odds are $\approx 1/\log n$.

Results for transitive subgroups

- $I(n, \nu)$:= proportion of σ fixing a partition of $[n]$ into ν equal blocks.
- $i(n, \boldsymbol{k}, \boldsymbol{d})$:= proportion of σ fixing each set of a partition $(C_1, \ldots, C_r)$ of $[n]$, with $|C_i| = k_i$ and $\sigma\big|_{C_i}$ consisting of d_i-divisible cycles.

Results for transitive subgroups

- $I(n,\nu)$:= proportion of σ fixing a partition of $[n]$ into ν equal blocks.
- $i(n,\boldsymbol{k},\boldsymbol{d})$:= proportion of σ fixing each set of a partition $(C_1,\ldots,C_r)$ of $[n]$, with $|C_i| = k_i$ and $\sigma\big|_{C_i}$ consisting of d_i-divisible cycles.

An easy reduction: $I(n,\nu) \asymp_\nu i(n,(\underbrace{n/\nu,\ldots,n/\nu}_{\nu-d \text{ times}},dn/\nu),(\underbrace{1,\ldots,1}_{\nu-d \text{ times}},d))$

for some d. Moreover, $d=1$ if $\nu \le 4$, and $d=\nu-1$ if $\nu \ge 5$.

Results for transitive subgroups

- $I(n,\nu)$:= proportion of σ fixing a partition of $[n]$ into ν equal blocks.
- $i(n,\boldsymbol{k},\boldsymbol{d})$:= proportion of σ fixing each set of a partition $(C_1,\dots,C_r)$ of $[n]$, with $|C_i| = k_i$ and $\sigma\big|_{C_i}$ consisting of d_i-divisible cycles.

An easy reduction: $I(n,\nu) \asymp_\nu i(n, (\underbrace{n/\nu,\dots,n/\nu}_{\nu-d \text{ times}}, dn/\nu), (\underbrace{1,\dots,1}_{\nu-d \text{ times}}, d))$

for some d. Moreover, $d = 1$ if $\nu \le 4$, and $d = \nu - 1$ if $\nu \ge 5$.

Theorem (Eberhard, Ford, K. (2016))

Let $\nu | n$, $1 < \nu < n$. Then

$$I(n,\nu) \asymp \begin{cases} n^{-\delta_\nu}(\log n)^{-3/2} & \text{if } 2 \le \nu \le 4, \\ n^{-1+1/(\nu-1)} & \text{if } 5 \le \nu \le \log n, \\ n^{-1} & \text{if } \log n \le \nu \le n/\log n, \\ n^{-1+\nu/n} & \text{if } n/\log n \le \nu < n. \end{cases}$$

Results for transitive subgroups, ctd.

- $T(n)$:= proportion of σ in some transitive $G \leq S_n$, $G \neq A_n, S_n$;
- $P(n)$ as above, with G primitive transitive.

Results for transitive subgroups, ctd.

- $T(n)$:= proportion of σ in some transitive $G \leq S_n$, $G \neq A_n, S_n$;
- $P(n)$ as above, with G primitive transitive.

Theorem (Eberhard, Ford, K. (2016))

$P(n) \leq n^{-1+o(1)}$

(This improves on previous work of Bovey and Diaconis-Fulman-Guralnik, who had $P(n) \leq n^{-2/3+o(1)}$.)

Results for transitive subgroups, ctd.

- $T(n)$:= proportion of σ in some transitive $G \leq S_n$, $G \neq A_n, S_n$;
- $P(n)$ as above, with G primitive transitive.

Theorem (Eberhard, Ford, K. (2016))

$P(n) \leq n^{-1+o(1)}$

(This improves on previous work of Bovey and Diaconis-Fulman-Guralnik, who had $P(n) \leq n^{-2/3+o(1)}$.)

Theorem (Eberhard, Ford, K. (2016))

If p is the smallest prime factor of n, then

$$T(n) \asymp \begin{cases} n^{-\delta_2}(\log n)^{-3/2} & \text{if } p = 2, \\ n^{-\delta_3}(\log n)^{-3/2} & \text{if } p = 3, \\ n^{-1+1/(p-1)} & \text{if } 5 \leq p \ll 1, \\ n^{-1+o(1)} & \text{if } p \to \infty. \end{cases}$$

Thank you!