Hunting Cycles in Permutation Groups

Cheryl E Praeger

21 / June / 2022

10th Edition: Ischia Group Theory 2022, Ischia

Heartfelt thanks to:

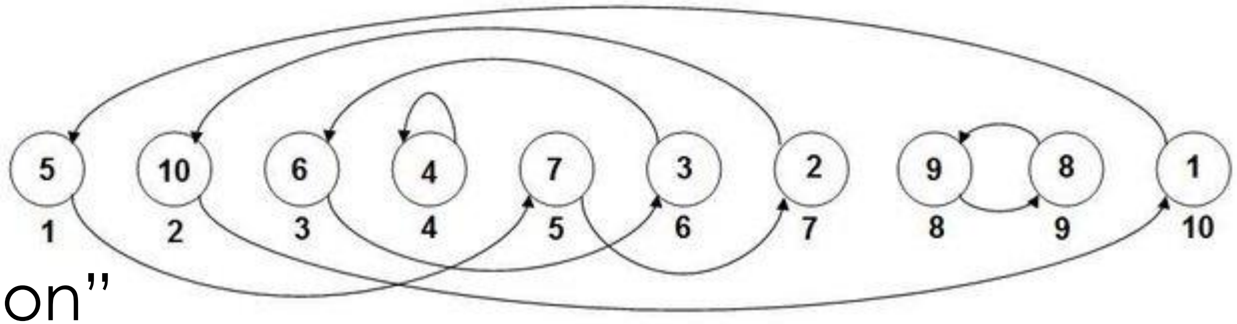
Mariagrazia Bianchi,
Andrea Caranti,
Patrizia Longobardi,
Mercede Maj and
Carlo Scoppola.

This lecture: hunting cycles

1. Which ones are interesting/useful?
2. How to find them and use them

Standard kinds of cycles in permutation groups

- Example $\Omega = \{1, \dots, 10\}$
- Write "disjoint cycle representation"
- Represent: $g = (1,5,7,2,10)(3,6)(4)(8,9)$
- Sometimes: "g is a cycle" means it has just one nontrivial cycle



Product of 4 cycles
Often omit fixed point (4)
(cycle of length 1)

What kinds of permutation groups?

Permutation groups on $\Omega = \{1, 2, \ldots, n\}$

Symmetric group $S_n = \{$ all permutations on $\Omega\}$

Alternating group $A_n = \{$ all even permutations on Ω $\}$

(products of an even number of 2-cycles) A_n simple if $n \geq 5$

Define permutation group $G \leq S_n$ to be transitive:

for all $i, j \in \Omega$, there exists $g \in G$ such that $g : i \to j$.

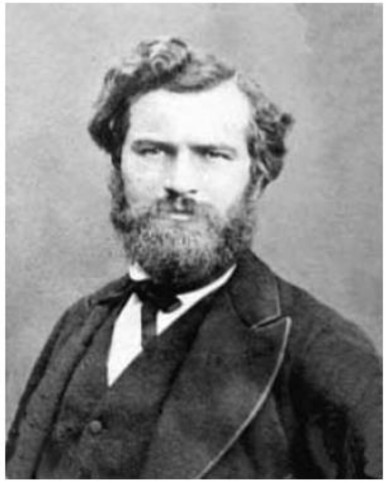
S_n and A_n are the giants among permutation groups on Ω

- Transitive permutation group primitive:
- Only trivial invariant partitions
- Stabilisers are maximal subgroups

Why care about cycles in permutation groups?

Theorem: Camille Jordan $\sim$ 1870

Given transitive $G \leq S_n$ and prime p such that $n/2 < p \leq n-3$ and some element of G contains a p-cycle; then G is A_n or S_n

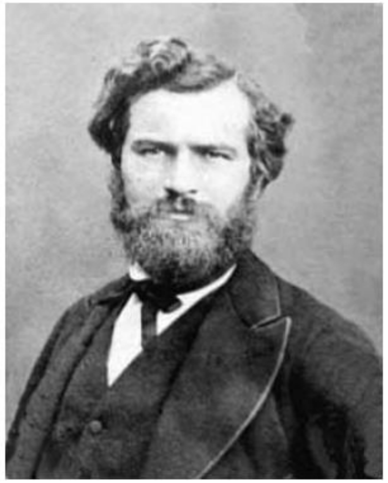


- Famous old result
- Highlights the giants S_n and A_n

Why care about cycles in permutation groups?

Theorem: Camille Jordan ∼ 1870

Given **primitive** $G \le S_n$ and prime p such that $n/2 < p \le n-3$ and some element of G **is** a p-cycle; then G is A_n or S_n



- Previous version follows from this
- Highlights the giants S_n and A_n

Why care about cycles in permutation groups?

THE UNIVERSITY OF WESTERN AUSTRALIA

- chasing up early 20C extensions of Jordan’s theorem
- Identified other elements of prime order such that the only primitive groups containing them are the giants
- Best results up to 1920 were by W. A. Manning

- I’ve been involved with permutation groups since my doctoral work

Primitive permutation group $G \leq S_n$

THE UNIVERSITY OF WESTERN AUSTRALIA

- Suppose exists $g \in G$ prime order p
- With q cycles of length p and f fixed points so $n = qp + f$
- Jordan/Manning: if $q \leq 5$ and $f > q + 1$

Then G is a giant S_n or A_n

- Manning (1918): if $5 < q \leq (p-1)/2$ and $f > 4q - 4$

Then G is a giant S_n or A_n

- I've been involved with permutation groups since my doctoral work

Primitive permutation group G < Sn

- Suppose exists $g \in G$ prime order p

- With q cycles of length p and f fixed points so $n = qp + f$

- CEP 1979: if $q \leq p - 1$ and $f > 5q/2 - 2$

Then G is a giant $\mathrm{S_n}$ or $\mathrm{A_n}$ or a "giant on pairs" $\mathrm{S_c}$ or $\mathrm{A_c}$ with $n = c(c-1)/2$

- I've been involved with permutation groups since my doctoral work

Primitive permutation group G < Sn

- Suppose exists $g \in G$ prime order p
- With q cycles of length p and f fixed points so $n = qp + f$
- Liebeck & Saxl 1985: if $q \leq p - 1$ then all possible G, p, q, f are known [in a long list]

- After this result methods/results changed because of the finite simple group classification

Primitive permutation group G < Sn

- Some "algorithmic-specific" uses of cycles: **which permutations determine giants (cf. Jordan) and are easy to find?**

- In 1970's many discussions with John Cannon. Using Jordan's result computationally to test whether a given primitive group $G = \langle X \rangle \leq S_n$ was a giant.

- Why? Existing algorithms for primitive groups efficient EXCEPT for giants.

- Reason for talking about these results was to say: permutation cycles were high in my consciousness as a young researcher

Primitive permutation group $G = \langle X \rangle \leq S_n$

- Example: $g = (13745)(689)$ is a witness in S_9 for both $p = 5$ and $p = 3$ since $g^3 = (14357)$; and $g^5 = (698)$ [same g more than one p]

- Example: $g = (13)(245689)$ in S_{11} gives $g^2 = (258)(469)$ with $p = 3$, q=2, f=5 > q+1; [Jordan/Manning result]

- Kind of processing? How much is realistic?

- What kinds of witnesses for G being a giant?

Primitive permutation group $G = \langle X \rangle \leq S_n$

THE UNIVERSITY OF WESTERN AUSTRALIA

Complete processing: For each prime p dividing length of some g–cycle examine element $g^{|g|/p}$ of order p in $\langle g \rangle$

- Decide if $g^{|g|/p}$ is a witness, using any of the previous results

- Issues:
  - Complicated to implement
  - Do some (simple) types of elements occur so frequently you would not bother with the other types

- Don't compute $g^{|g|/p}$
- Just look at cycle lengths
- Still it's rather messy

Simple Algorithm using only Jordan's theorem

THE UNIVERSITY OF WESTERN AUSTRALIA

Define $g \in S_n$ is 'good' if g contains a p-cycle, for some prime p such that $n/2 < p \leq n-3$

Example: $g = (12345)(67) \in S_9$ is 'good': $n = 9, p = 5$

For fixed p, number of elements in S_n containing a p-cycle is

$$\binom{n}{p}(p-1)!(n-p)! = \frac{n!}{p} \quad \left(\text{and} \quad \frac{n!}{2p} \quad \text{in } A_n\right)$$

Proportion of 'good' elements in A_n or S_n

$= \sum_{n/2<p\leq n-3} \frac{1}{p} \geq \frac{c}{\log n}$ for some constant c

- If $p > n/2$ then no overlap between different primes
- Proportion good elts **equals** O(log n)
- So O(log n) random elements finds 'good' element with high probability

Better use of Jordan's theorem to recognize giants?

- O(log n) random elements finds 'good' element with high probability
- **Can we make do with fewer random elements?**
- Jordan: finding a p-cycle for any prime p is OK/decisive witness that primitive G is a giant

Why bother?

- Imagine you feed a non-giant to this procedure: won't stop until log n elements processed

Better use of Jordan's theorem to recognize giants?

THE UNIVERSITY OF WESTERN AUSTRALIA

- Elements g yielding p-cycle:

$$g = (p - cycle) \ldots (coprime\ to\ p)$$

- E.g. g=(12345)(65)(8,9,10) etc
- Call these elements **pre p-cycles**
- What is proportion of pre p-cycles (for some p) in S_n?
- Is it c/log n or is it asymptotically larger?

- Know: proportion of pre p-cycles for some p>n/2 is c/log n

Proportion from "small" primes

- 2018 John Bamberg, Stephen Glasby, Scott Harper, CEP: Our first attempt

- Fixed prime p as $n \to \infty$: proportion of pre p-cycles grows like $c(p)(n/p)^{-1/p}$

- Problem: even adding over(bounded) $p \leq K$ (ignoring any overlap) only get proportion $cn^{-1/K}$

- What we learned: contribution from bounded p is too small

- For small primes the sets of pre p-cycles for different p intersect
- recall: $g = (13745)(689)$
- Powers to 5-cycle and to a 3-cycle

Proportion of pre p-cycles for what primes p?

- Erdos and Turan: holds clues about most prevalent elements of S_n: they have $\approx \log n$ cycles, but what are their lengths?
- Stephen Glasby and I struggling over this

Proportion of pre p-cycles for what primes p?

THE UNIVERSITY OF WESTERN AUSTRALIA

- Erdos and Turan: holds clues about most prevalent elements of S_n: they have $\approx \log n$ cycles, but what are their lengths?
- Stephen Glasby and I struggling over this when
- Bill Unger arXiv May 2019 :

"Almost all permutations power to a prime length cycle"

  - Asymptotic result – great insights – unclear where these "almost all permutations" being pre p-cycles were hiding – for what primes p?

Understanding where the "bulk" of the proportion lay required more delicate analysis

Proportion of pre p-cycles for what primes p?

Stephen Glasby, Bill Unger and I joined forces:

- Focused on prime $p \approx \log n$:
  - Needed to consider $\approx \log n$ different primes p
  - Reverse engineer using the Prime Number Thm
  - primes p between $\log n$ and $(\log n)^{\log\log n}$
  - Plenty of scope for overlap between sets of pre p-cycles for different p
  - So very delicate analysis needed

- My conviction: primes p giving large contribution should be roughly $p \approx \log n$

Proportion of pre p-cycles for these primes p

2021 Stephen Glasby, Bill Unger, CEP:

- Proportion of elements of S_n that are pre p-cycles for some prime p between $\log n$ and $(\log n)^{\log\log n}$ is at least

$$1 - \frac{5}{\log\log n}$$

For proportion in A_n change 5 to 7

- For computational use we also proved
  - Proportion of pre p-cycles in S_n (for some p) is at least $\frac{1}{19}$

Precise computations: for $n \leq 50$ show proportion > 1/3

Strategy of proof

THE UNIVERSITY OF WESTERN AUSTRALIA

Need to estimate size of the union

Pre(n) = set of all pre-p-cycles for all primes $\boldsymbol{p \in P(n)}$

where $P(n) = \{\, p \mid \log n \leq p \leq (\log n)^{\log\log n} \,\}$

- **Strategy: $\mathbf{Pre(n)}$** contains $T(n) \setminus U(n)$ where
- T(n) is the too large set

$$T(n) = \{\, g \in S_n \mid g \; has \; at \; least \; one \; p - cycle \; for \; some \; p \in P(n)\}$$

- U(n) is the unwanted set $U(n) = \cup_{p \in P(n)} \mathrm{U(p)}$, where

$$U(p) = \{\, g \in S_n \mid g \; has \; at \; least \; one \; p - cycle \; \& \; also \; a \; second \; cycle \; of \; length \; a \; multiple \; of \; p\}$$

Strategy of proof 2

THE UNIVERSITY OF WESTERN AUSTRALIA

Checking properties:

1. $T(n) = \{ g \in S_n \mid g \text{ has at least one } p - \text{cycle for some } p \in P(n)\}$ implies that $Pre(n) \subseteq T(n)$
2. $U(n) \cup_{p \in P(n)} U(p)$, *where* $U(p) = \{ g \in S_n \mid g \text{ has at least one } p - \text{cycle \& also a second cycle of length a multiple of } p\}$

Implies that each $g \in T(n) \setminus U(n)$ is a pre-p-cycle for some p in P(n), and hence lies in Pre(n).

Hence $\boldsymbol{Pre(n)}$ contains $T(n) \setminus U(n)$

- Note, inclusion proper: U(n) might contain an element of some U(p) if it is a pre p'-cycle for some other p' in P(n) ☺

Strategy of proof 3

THE UNIVERSITY OF WESTERN AUSTRALIA

Need a lower bound for $|\boldsymbol{Pre(n)}| \geq |T(n)| - |U(n)|$

- First: find lower bound for $\frac{|T(n)|}{n!} = 1 - \frac{|S(n)|}{n!}$

  Where $S(n) = \{ g \in S_n \text{ has no cycles length } p \text{ for any } p \in P(n)\}$

- So we need upper bound for $|S(n)|$
- This is a "forbidden cycle lengths" question solved by Erdos and Turan: $\frac{|S(n)|}{n!} \leq \mu$
- Unfortunately the E-T upper bound becomes $\mu \approx log\ log\ n$ for P(n)
- We improve this to $\frac{|S(n)|}{n!} \leq 2.3/\log\log n$ so $\frac{|T(n)|}{n!} \geq 1 - 2.3/\log\log n$

Strategy of proof 4

THE UNIVERSITY OF WESTERN AUSTRALIA

Second: find an upper bound for $|U(n)|$

- $U(n) = \cup_{p\in P(n)} U(p)$ and we estimate this by $|U(n)| \leq \sum_{p\in P(n)} |U(p)|$
- Very delicate estimates involving $\sum_{p\in P(n)} \frac{1}{p^2}$
- End up with $\frac{|U(n)|}{n!} \leq \frac{2.2}{\log\log n}$
- So our proportion of pre p-cycles for p in P(n) is at least

$$\frac{|T(n)|}{n!} - \frac{|U(n)|}{n!} \geq 1 - \frac{2.3}{\log\log n} - \frac{2.2}{\log\log n} > 1 - \frac{5}{\log\log n}$$

Qed ☺

Where did the idea for primes around log n come from?

THE UNIVERSITY OF WESTERN AUSTRALIA

- Ideas for recognizing giant primitive groups influenced recognition algorithms for finite classical matrix groups

- Equivalents of p-cycles we currently call stingray elements: relative to an appropriate basis they look like:

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$$ with A irreducible in GL(r,q)

- Sometimes we take |A| a ppd prime divisor of $q^r - 1$
- To allow effective application of FSGC

Where did the idea for primes around log n come from?

- stingray elements: in GL(n,q)

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$$ with A irreducible in GL(r,q)

- 1992: Neumann—Praeger SL-recognition algorithm used r = n, and r = n-1
- 1998: Niemeyer—Praeger classical recognition algorithm used any r > n/2

- Much influenced by Jordan elements in Sn

Where did the idea for primes around log n come from?

THE UNIVERSITY OF WESTERN AUSTRALIA

- stingray elements: in GL(n,q)

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$$ with A irreducible in GL(r,q)

- Early 2000's: Seress experimenting with new recognition algorithm suggested used r roughly log n

- 2014: Niemeyer—Praeger With probability c/log n, a random element in Class(n,q) powers to a stingray with log n < r < 2log n [this influenced my thinking about "what p" for pre p-cycles]

- Aachen PhD student Daniel Rademacher:
- designing and analysing the corresponding classical recognition algorithm

References for recent results

THE UNIVERSITY OF WESTERN AUSTRALIA

2020 John Bamberg, Stephen Glasby, Scott Harper, CEP

Permutations with orders coprime to a given integer,

Electronic J. Combin. **27**, P1.6

2021 Stephen Glasby, CEP, William R. Unger

Most permutations power to a cycle of small prime length,

Proc. Edin. Math. Soc. **64**, 234-246.

2014 Alice C. Niemeyer, CEP

Elements in finite classical groups whose powers have large 1-Eigenspaces [Corollary 3.5]

Disc. Math. and Theor. Comp. Sci. **16**, 303-312.