

# Probability a Group Element is Pivotal

David Housman

Goshen College

MAA Indiana Section Spring 2024 Meeting

These slides can be downloaded from [www.goshen.edu/dhousman](http://www.goshen.edu/dhousman)  
under the Presentations section

Choose elements of a group at random one at a time without replacement. When the elements chosen first generate the group, the last chosen element is called *pivotal*. We determine the probability that an element is pivotal in a few groups and show some dismal attempts to get some help from ChatGPT. I am hopeful that algebraists, probabilists, and linguists can provide some helpful suggestions for further steps or direct me to the literature where the question has already been answered.

# A Simple Example

- 1 Consider  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$  with addition modulo 6.
  - Randomly select 2.  $\langle 2 \rangle = \{0, 2, 4\}$ ; hence, 2 is not pivotal.
  - Randomly select 4.  $\langle 2, 4 \rangle = \{0, 2, 4\}$ ; hence, 4 is not pivotal.
  - Randomly select 3.  $\langle 2, 3, 4 \rangle = \{0, 1, 2, 3, 4, 5\}$ ; hence, 3 is pivotal.
- 2 The only proper subgroups of  $\mathbb{Z}$  are  $\langle 2 \rangle = \{0, 2, 4\}$  and  $\langle 3 \rangle = \{0, 3\}$ .
- 3 Element 1 is pivotal if it comes after (and occurs with probability):
  - nothing (prob =  $\frac{1}{6}$ )
  - one of 0, 2, 3, or 4 (prob =  $\frac{4}{6} \frac{1}{5}$ )
  - two of 0, 2, or 4 (prob =  $\frac{3}{6} \frac{2}{5} \frac{1}{4}$ )
  - 0 and 3 (prob =  $\frac{2}{6} \frac{1}{5} \frac{1}{4}$ )
  - 0, 2, and 4 (prob =  $\frac{3}{6} \frac{2}{5} \frac{1}{4} \frac{1}{3}$ )
- 4 The probability 1 is pivotal is  $\frac{20+16+6+2+2}{120} = \frac{46}{120}$ .
- 5 0, 1, 2, 3, 4, 5 pivotal probabilities:  $\frac{0}{120}, \frac{46}{120}, \frac{6}{120}, \frac{16}{120}, \frac{6}{120}, \frac{46}{120}$ .
- 6  $120 = 5!$ , the number of permutations of the non-zero elements.

# General Problem

- 1 A *group* is a set  $G$  and a binary operation  $*$  satisfying
  - (closure) if  $x, y \in G$ , then  $x * y \in G$ ;
  - (identity) there is an  $e \in G$  satisfying  $e * x = x * e = x$  for all  $x \in G$ ;
  - (inverses) if  $x \in G$ , then there is an  $x^{-1} \in G$  satisfying  $x * x^{-1} = x^{-1} * x = e$ ; and
  - (associativity) if  $x, y, z \in G$ , then  $x * (y * z) = (x * y) * z$ .
- 2 The set  $H \subset G$  is a *subgroup* of  $G$  if  $H$  is a group.
- 3 Given the set  $S \subset G$ , the *generating subgroup*  $\langle S \rangle$  is the smallest subgroup of  $G$  that contains  $S$ .
- 4 Suppose a group  $G$  has  $n$  elements. An *ordering* of  $G$  is a one-to-one and onto function  $o : \mathbb{Z}_n \rightarrow G$ , and element  $y = o(j) \in G$  is *pivotal* for  $\alpha$  if  $\langle o(0), \dots, o(j-1) \rangle \neq G$  and  $\langle o(0), \dots, o(j) \rangle = G$ .
- 5 The *pivotal probability* of the element  $x$  of a group  $G$  with  $n$  elements, denoted  $\phi_x(G)$  or  $\phi_x$ , is the number of orderings of  $G$  in which  $x$  is pivotal divided by  $n!$ .

## Two General Results

### Theorem

*If  $e$  is the identity element of the group  $G$ , then  $\phi_e = 0$ .*

**Proof.** For any  $S \subset G$ ,  $e \in \langle S \rangle$ . So,  $\langle S \rangle = \langle S \cup \{e\} \rangle$ . Thus, adding  $e$  to any set of non-generating elements does not change it into a generating set. Therefore,  $e$  is never pivotal.

### Theorem

*If  $\alpha$  is an automorphism of the group  $G$ , then  $\phi_x = \phi_{\alpha(x)}$ .*

**Proof.** The automorphism  $\alpha$  can be used to define a bijective map from group  $G$  element lists  $(x_1, x_2, \dots, x_n)$  onto group  $G$  element lists  $(\alpha(x_1), \alpha(x_2), \dots, \alpha(x_n))$ ; hence,  $x \in G$  is pivotal in the ordering  $(x_1, x_2, \dots, x_n)$  if and only if  $\alpha(x)$  is pivotal in the ordering  $(\alpha(x_1), \alpha(x_2), \dots, \alpha(x_n))$ .

## Theorem

If  $G = \mathbb{Z}_n$  where  $n = p^m$ ,  $p$  is prime, and  $m$  is a positive integer, then

$$\phi_x(G) = \begin{cases} \frac{1}{p^{m-1}(p-1)} & \text{if } \gcd(x, n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

**Proof.** Let  $H = \langle p \rangle$ .

So,  $|H| = p^{m-1} = n/p$ , and

$$|G - H| = n - n/p = p^m - p^{m-1} = p^{m-1}(p - 1).$$

A set  $S \subset G$  is generating iff  $S \cap (G - H) \neq \emptyset$ .

An element  $x$  is pivotal iff  $x \in G - H$  is chosen before any of the other elements in  $G - H$ .

# Cyclic Groups II

## Theorem

If  $G = \mathbb{Z}_n$  where  $n = pq$  and  $p \neq q$  are prime, then

$$\phi_x(G) = \frac{1}{n-1} \begin{cases} (q-1)/(n-q) & \text{if } x \in \langle p \rangle - \{0\} \\ (p-1)/(n-p) & \text{if } x \in \langle q \rangle - \{0\} \\ 1 + \frac{p-1}{n-p} + \frac{q-1}{n-q} & \text{if } x \in G - \langle p \rangle - \langle q \rangle \\ 0 & \text{if } x = 0 \end{cases}$$

**Proof.** An element  $x \in \langle p \rangle - \{0\}$  is pivotal iff one or more elements from  $\langle q \rangle - \{0\}$  appear before  $x$  and no other non-identity elements appear before  $x$ . An element  $x \in \langle q \rangle - \{0\}$  is analogous. An element

$x \in G - \langle p \rangle - \langle q \rangle$  is pivotal iff  $x$  is the first non-identity element, the elements before  $x$  are a nonempty subset of  $\langle p \rangle - \{0\}$ , or the elements before  $x$  are a nonempty subset of  $\langle q \rangle - \{0\}$ .

# Dihedral Groups

## Theorem

If  $G = D_p$ , where  $p$  is prime, is the group of symmetries of a regular  $p$ -gon, then

$$\phi_R = \frac{p}{2p-1} \frac{1}{2p-2} \quad \text{and} \quad \phi_F = \frac{p-1}{2p-1} \frac{1}{2p-2} + \frac{p-1}{2p-1} \frac{1}{p}$$

if  $R$  is a non-identity rotation and  $F$  is a reflection.

**Proof.** Any two distinct reflections and any reflection with any non-identity rotation forms a minimal generating set, and these are all of the minimal generating sets.

A non-identity rotation  $R$  is pivotal iff exactly one reflection appears before  $R$ .

A reflection  $F$  is pivotal iff (a) exactly one other reflection appears before  $F$ , or (b) one or more non-identity rotations appear before  $F$  and  $F$  is the first reflection to appear.

# An Alternating Group

## Theorem

If  $G = A_4$  is the group of even permutations of  $\{1, 2, 3, 4\}$ , then

$$\phi_{(i,j,k)} = 25/264 \approx 0.095 \quad \text{and} \quad \phi_{(ij)(kl)} = 8/99 \approx 0.081.$$

**Proof.** There are two non-identity types of elements: eight 3-cycles  $(ijk)$  and three 2-cycle pairs  $(ij)(kl)$ .

The element  $(123)$  is pivotal iff it is preceded by (a) a nonempty subset of the 2-cycle pairs, (b) a 3-cycle not equal to  $(132)$ , or (c) a 3-cycle not equal to  $(132)$  and its square. Thus,  $\phi_{(123)} = \frac{3}{11} \frac{1}{8} + \frac{6}{11} \frac{1}{10} + \frac{6}{11} \frac{1}{10} \frac{1}{9}$ .

The element  $(12)(34)$  is pivotal iff it is preceded by (a) a 3-cycle, or (b) a 3-cycle and its square. Thus,  $\phi_{(12)(34)} = \frac{8}{11} \frac{1}{10} + \frac{8}{11} \frac{1}{10} \frac{1}{9}$ .

- Me: List the minimal generating sets for  $\mathbb{Z}_6$ .
- Wolfram: The minimal generating sets for  $\mathbb{Z}_6$  (which is isomorphic to the cyclic group  $C_6$ ) are given by the elements that generate the entire group. In the case of  $\mathbb{Z}_6$ , these elements are 1 and 5, as each of these elements can generate all elements of  $\mathbb{Z}_6$  through their multiples modulo 6.
- Me: The set  $\{2,3\}$  is also a minimal generating set for  $\mathbb{Z}_6$ .
- Wolfram: You are correct, and I appreciate your patience. The set  $\{2,3\}$  is indeed a minimal generating set for  $\mathbb{Z}_6$ . In a group like  $\mathbb{Z}_6$ , which is cyclic and has 6 elements, any set of elements that can together generate all the elements of the group can be considered a generating set. The elements 2 and 3, through their multiples and combinations, can generate all elements of  $\mathbb{Z}_6$ , thus qualifying as a minimal generating set. Thank you for pointing this out.

- Me: Can you now list all minimal generating sets for  $\mathbb{Z}_6$ ?
- Wolfram: [Many words but the answer is  $\{1\}$ ,  $\{5\}$ , and  $\{2, 3\}$  closing with the following that suggests an understanding of minimality.]  
These sets are minimal in the sense that removing any element from them would result in a set that no longer generates the entire group.
- Me: Are there more such sets?
- Wolfram: The search did not yield specific information about all minimal generating sets for  $\mathbb{Z}_6$  within the provided documents. However, .... While  $\{1\}$ ,  $\{5\}$ , and  $\{2, 3\}$  are clear examples, there might not be other sets that meet the criteria for minimal generating sets in  $\mathbb{Z}_6$ . ... The elements 0, 4, and 6 (which is equivalent to 0 in this group) do not contribute to generating the group due to their order. Therefore, it seems that we have covered the minimal generating sets for  $\mathbb{Z}_6$ .

# ChatGPT 4.0 with Wolfram

- Me: Is  $\{2,4\}$  a minimal generating set for  $\mathbb{Z}_6$ ?
- Wolfram: The set  $\{2,4\}$  cannot be a minimal generating set for  $\mathbb{Z}_6$ . In a group like  $\mathbb{Z}_6$ , a generating set must be able to produce all elements of the group through combinations of its elements and their multiples. The element 2 generates  $\{0, 2, 4\}$  and the element 4, which is congruent to  $-2 \pmod{6}$ , generates the same set  $\{0, 2, 4\}$  when considering multiples modulo 6. Therefore, the set  $\{2,4\}$  can only generate a subset of  $\mathbb{Z}_6$  and not the entire group, making it not a generating set, and hence not a minimal generating set.
- Me: Is  $\{3,4\}$  a minimal generating set for  $\mathbb{Z}_6$ ?
- Wolfram: The set  $\{3,4\}$  is not a minimal generating set for  $\mathbb{Z}_6$ . [Argues that 3 generates  $\{0, 3\}$  and 4 generates  $\{0, 2, 4\}$ .] While the combination of 3 and 4 can generate a few more elements of  $\mathbb{Z}_6$  than either can individually, they cannot generate the entire group. Specifically, they cannot generate the element 1 ...

# ChatGPT 4.0 with Wolfram

- Me:  $\{3, 4\}$  can generate 1 because  $3 + 4 = 1$  in  $\mathbb{Z}_6$ .
- Wolfram: You are correct, and I appreciate your clarification. In  $\mathbb{Z}_6$ , the operation is addition modulo 6, and indeed,  $3 + 4 \equiv 1 \pmod{6}$ . Therefore, the set  $\{3, 4\}$  can generate 1, and from 1, every other element of  $\mathbb{Z}_6$  can be generated through multiples of 1. This means  $\{3, 4\}$  is indeed a minimal generating set for  $\mathbb{Z}_6$ , as it can produce all the elements of the group through the combination of its elements and their multiples. Thank you for pointing this out.
- Me: Can you now list all minimal generating sets for  $\mathbb{Z}_6$ ?
- Wolfram:  $\{\{1\}, \{5\}, \{2, 3\}, \text{ and } \{3, 4\}\}$  are listed with some argument for why each is a generating set. Then it states that these sets are minimal. Finally it notes that sets such as  $\{3, 4\}$  are "counterintuitive", but this is a step up from other ChatGPT versions that kept forgetting previous statements.]

# ChatGPT 4.0 with Wolfram

- Me: What are all the minimal generating sets for  $\mathbb{Z}_{10}$ ?
- Wolfram:  $\{\{1\}, \{3\}, \{7\}, \text{ and } \{9\}\}$  "are" the minimal generating sets.]
- Me: But  $\{4,5\}$  also generates all of  $\mathbb{Z}_{10}$  and no subset generates all of  $\mathbb{Z}_{10}$ . So, I would call  $\{4, 5\}$  a minimal generating set for  $\mathbb{Z}_{10}$ .
- Wolfram: You've made a valid point ... when combining 4 and 5, we can obtain 9 (as  $4 + 5 \equiv 9 \pmod{10}$ ), and subsequently 1 (as  $9 + 2 \equiv 1 \pmod{10}$ , where 2 is obtained from the multiples of 4), which can then generate the entire group. [The minimal generating sets now "include" the five sets obtained so far.]
- Me: Are there any other minimal generating sets for  $\mathbb{Z}_{10}$ ?
- Wolfram: [Many words] Given this, the sets listed above are likely the minimal generating sets for  $\mathbb{Z}_{10}$ . If there are others, they would have to be combinations of non-generators that uniquely generate all elements of  $\mathbb{Z}_{10}$  without any subset of them being able to do so, which is not apparent beyond the sets we've identified.

# ChatGPT 4.0 with Wolfram

- Me: Can you try checking other subsets?
- Wolfram: [Many words followed by three examples]
  - A set like  $\{2, 3\}$  could be considered, where 3 is a generator, making the set not minimal since 3 alone generates the entire group.
  - A set like  $\{2, 5\}$  might seem promising since 5 gives us an element not reachable by 2 alone, but since 5's order is 2, it only generates  $\{0, 5\}$ , and combined with 2, it cannot generate all elements. [Me: ChatGPT's confidence in stating falsehoods is amazing!]
  - A set like  $\{4, 6\}$  could also be considered, but since 4 and 6's orders divide 10, they may not cover all elements without including a generator, which again would not make the set minimal.

Given these considerations, it appears that aside from the individual generators and the  $\{4, 5\}$  set, other combinations either include a generator (making them non-minimal) or do not cover all elements of  $\mathbb{Z}_{10}$ . Therefore, the list provided earlier might encompass all the minimal generating sets for  $\mathbb{Z}_{10}$ , considering the constraints for a set to be minimal and generating in the context of a cyclic group.

- Me: What about  $\{5, 6\}$ ?
- Wolfram: [Argues why  $\{5, 6\}$  is a minimal generating set.]
- Me: Can you check every other subset of  $\mathbb{Z}_{10}$  to determine which ones are minimal generating?
- Wolfram: [Many words.] Given the limitations of this platform, conducting such an exhaustive check here is not feasible. However, the approach would involve systematically combining elements and checking if the set generated by their combinations covers  $\mathbb{Z}_{10}$ . This would be a combinatorial task, potentially suited for a more programmable environment where you can iterate over all subsets, check their generated sets, and filter out the minimal ones.

If you have access to computational software or a programming environment, I can guide you on how to set up such a check.

- Me: Could you write code for SageMath that would carry out this check?
- Wolfram: [Generally good code except for the following.]

```
def generates_Z10(subset):  
    generated = set(subset)  
    for a in subset:  
        for b in subset:  
            generated.add((a + b) % 10)  
    return set(range(10)) == generated
```

[`generates_Z10({4,5})` would create `generated` as  $\{0, 4, 5, 8, 9\}$  instead of  $\{0, 2, 3, 4, 5, 6, 7, 8, 9\}$ .]

# ChatGPT 4.0 with Wolfram

- Me: [After a few days.] Could you write code for SageMath that would carry out this check?
- Wolfram: [Generally good code except for the following.]

# Function to check if a set S is a generating set for  $Z_n$

```
def is_generating_set(S, n):  
    generated = set()  
    # Adding multiples of each element in S  
    for a in S:  
        for i in range(n):  
            generated.add((a*i) % n)  
    # Check if all elements of  $Z_n$  are generated  
    return generated == set(range(n))
```

[`is_generating_set({4,5}, 10)` would create `generated` as  $\{0, 2, 4, 5, 6, 8\}$  instead of  $\{0, 2, 3, 4, 5, 6, 7, 8, 9\}$ .]

- Me: Can you make the code more efficient by taking into account conjugacy classes?
- Wolfram: [After stating why conjugacy classes would not be helpful] A more relevant approach might involve the use of the greatest common divisor (gcd) to ensure elements have the potential to generate the group, alongside checking for the direct generation of the group without computing all multiples explicitly. [The revised code contained:]

```
# Function to check if a set S is a generating set for  $Z_n$ 
def is_generating_set(S, n):
    # Generate the subgroup by computing the gcd of n and
    subgroup_order = lcm([n // gcd(a, n) for a in S])
    # The set S generates  $Z_n$  if the subgroup order equals n
    return subgroup_order == n
```