Even and Odd Permutations

Ben O'Connell, Mark Dervan and Naoise O'Callaghan

MA3343 Groups Project

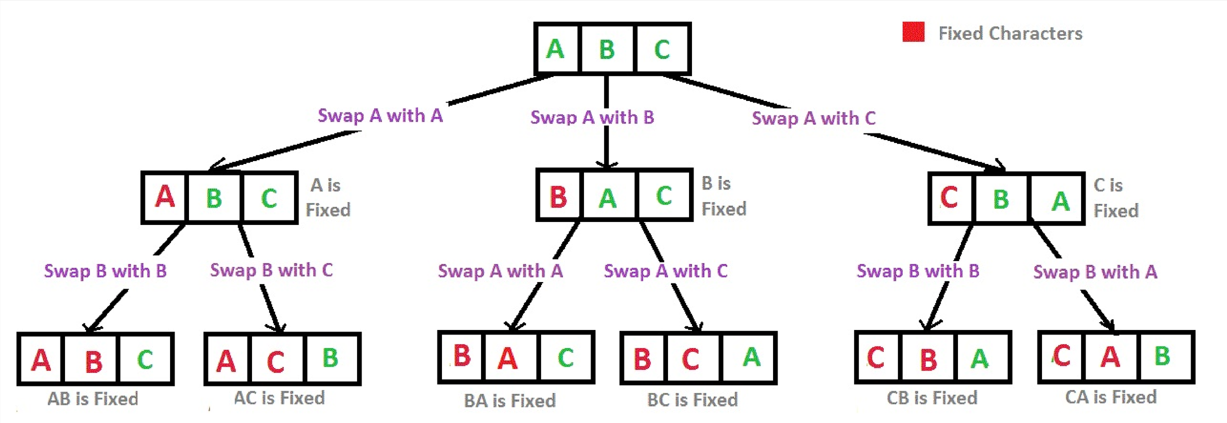
Introduction

A permutation can be defined as a rearrangement of an ordered list S in to a one-to-one correspondence with S itself.
The permutations of a set X = 1, 2, . . . , n form a group under composition. This group is called the symmetric group S_n of degree n.
A permutation is considered "even" if it can be written as a product of an even number of transpositions, it has sign +1.
Alternatively, a permutation is "odd" if it can be written as a product of an odd number of permutations, it has sign -1.

Objectives

The objective of this project is to teach the reader more about even and odd permutations while simultaneously proving the following three lemmas:

- Every permutation of a set 1,...n where n>2 can be written as a product of transpositions.
- Every permutation is either even or odd but never both.
- The group of even permutations form a subgroup of S_n however the odd permutations do not.



Recursion Tree for Permutations of String "ABC"

Writing permutations as a product of disjoint cycles.

Theorem: Every permutation of a finite set of n>1 elements can be written as a product of disjoint cycles.
Proof: Let α be a permutation of A = 1, 2, ...n. Pick any element, say a_1. This gets sent to a_2 as follows $\alpha(a_1) = a_2$, a_2 then gets sent to a_3 as follows $\alpha^2(a_1)$. As A is finite the sequence a_1, $\alpha(a_1)$, $\alpha^2(a_1)$,... must be finite and hence there must exist some i<j for which $\alpha^i(a_1) = \alpha^j(a_2)$ and m = j-i such that $a_1 = \alpha^m(a_1)$. We can write $\alpha = (a_1, a_2,...,a_m)$. If we have exhausted all elements of A then we're done. If not we pick some b_1 from the elements left and repeat the same process to get a cycle $(b_1, b_2,...,b_k)$. We note that the two cycles are disjoint. If they had elements in common then for some i and j we would have $\alpha(a_1) = \alpha(b_1)$, that is $b_1 = \alpha^{i-j}(a_1)$. This would imply b_1 is an element of the cycle $(a_1, a_2,...,a_m)$, which contradicts the way b_1 was chosen.We repeat this process until all elements of A are exhausted

Writing permutations as a product of transpositions

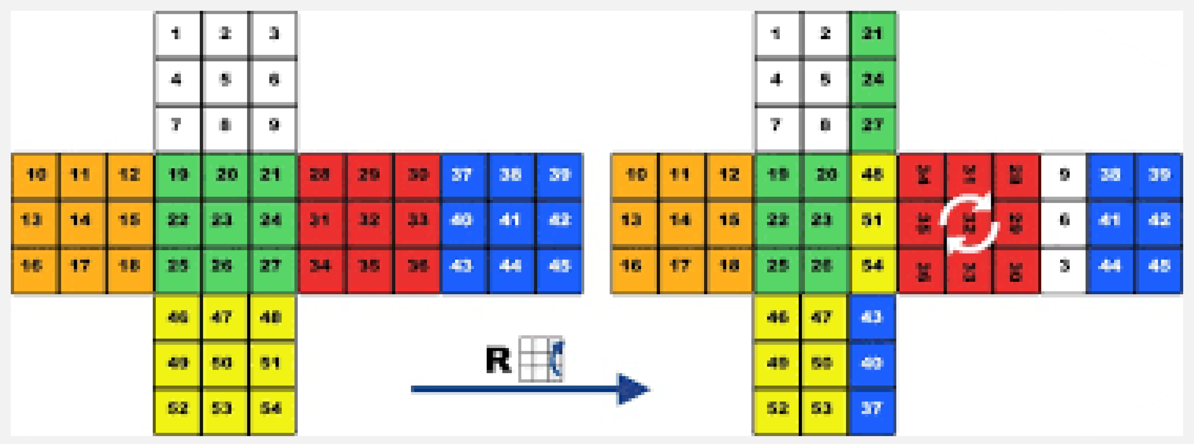
Each cycle in S_n with n>1 can easily be shown to be written as a product of transpositions. The cycle $(a_1, a_2,...,a_p)$ can be written as (a_1, a_p), (a_1, a_{p-1}), ... ,(a_1, a_3), (a_1, a_2).
We have shown that every permutation can be written as a product of disjoint cycles and also that any cycle in S_n with n>1 can be written as a product of permutations. It follows trivially that each permutation can be written as a product of transpositions.

Even and odd permutations

Prelude: The identity permutation on S_n, that is the permutation that sends every element to itself, is even.
Theorem: No permutation is both even and odd
Proof: Lets suppose α is both even and odd. So $\alpha = \beta_1\beta_2...\beta_m = \lambda_1\lambda_2...\lambda_n$ where m is even and m is odd. Since every transposition is its own inverse, this would imply that id= $\beta_1\beta_2...\beta_m\lambda_n\lambda_{n-1}...\lambda_1$. Since n+m is odd, this contradicts the fact that α is both even and odd.

Representing permutations as groups

As we stated earlier the permutations of a set X=[1, 2, . . . , n] form a group under composition. This group is called the symmetric group S_n of degree n.
Identity: Let s be a permutation of S_n clearly s ∘ id = id ∘ s = s, S_n contains the identity element, id.
Inverse: The inverse s^{-1} of s is a permutation of S_n by definition and s ∘ $s^{-1} = s^{-1}$ ∘ s.
Associative: Composition of functions is associative.
Closure: Multiplying two permutations, f and g, yields another permutation.



Group of even permutations as a subgroup of S_n

Clearly the set of even permutations, A_n, is a subset of S_n, the set of all permutations. We now show A_n is a group itself under the operation of composition.
Identity: Let s be a permutation of S_n clearly s ∘ id = id ∘ s = s, S_n contains the identity element, id. Here s is an even permutation.
Inverse: The inverse s^{-1} of s is a permutation of S_n by definition and s ∘ $s^{-1} = s^{-1}$ ∘ s.
Associative: Composition of functions is associative.
Closure: Multiplying two permutations, f and g, yields another permutation.

Group of odd permutations as a subgroup of S_n

Although the set of odd permutations is a subset of the set of all permutations it fails to be a subgroup of the group S_n as it does not contain the identity element. The identity element, id, is an even permutation and as we have previously shown a permutation cannot be both even and odd.

Real Life Applications

- Although a trivial example, we see permutation groups in the rubiks cube. We can rotate the 6 faces of the cube so we can define 6 basic operations or permutations which rearrange the ordered list in a certain way.
- Combination locks should technically be called "Permutation Locks" as they use permutations and not combinations.