CS 5319
Advanced Discrete Structure

Lecture 13:
Introduction to Group Theory III

Outline

- Introduction
- Groups and Subgroups
- Generators
- Cosets (and Lagrange's Theorem)
- Permutation Group (and Burnside's Theorem)
- Group Codes

Permutation Group

- Let S be a set with finite number of elements
- A one-to-one function from S onto itself is called a permutation
- We use the notation : $\begin{pmatrix} abcd \\ bdca \end{pmatrix}$

  to denote the permutation of the set { a, b, c, d } that maps a to b, b to d, c to c, and d to a
- Note: Elements in upper row can be in arbitrary order

Permutation Group

- Suppose the set S has n elements
- Let A denote the $n!$ permutations of S
- We define the binary operation $\circ$ on A to be the composition of two functions

Ex :

$$\begin{pmatrix} abcd \\ bdca \end{pmatrix} \circ \begin{pmatrix} abcd \\ acbd \end{pmatrix} = \begin{pmatrix} abcd \\ bcda \end{pmatrix}$$

Permutation Group

Lemma 1:

The binary operation $\circ$ on A is closed

Proof :

Let π_1 and π_2 be two permutations on S.

To show $\pi_1 \circ \pi_2$ is in A, we only need to show no two elements are mapped to the same element by $\pi_1 \circ \pi_2$ (why?)

Permutation Group

Proof (cont) :

Suppose π_2 maps a to b, and π_1 maps b to c

➔ $\pi_1 \circ \pi_2$ maps a to c

Now for any $x \neq a$, π_2 will map x to some y distinct from b (since π_2 is a permutation)

Similarly, π_1 will map y to some z distinct from c (since π_1 is a permutation)

➔ $\pi_1 \circ \pi_2$ will not map x to c

Permutation Group

Lemma 2:

The binary operation $\circ$ on A is associative

Proof :

Let π_1 , π_2 , and π_3 be three permutations on S.

Our target is to show

$$(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$$

Permutation Group

Proof (cont) :

Suppose that π_3 maps *a* to *b*, π_2 maps *b* to *c*, and π_1 maps *c* to *d*

We have $(\pi_1 \circ \pi_2)$ maps *b* to *d*

➔ $(\pi_1 \circ \pi_2) \circ \pi_3$ maps *a* to *d*

On the other hand, $(\pi_2 \circ \pi_3)$ maps *a* to *c*

➔ $\pi_1 \circ (\pi_2 \circ \pi_3)$ maps *a* to *d*

Thus $\circ$ is an associative operation

Permutation Group

Ex :

$$\pi_1 = \begin{pmatrix} abcd \\ adbc \end{pmatrix} \quad \pi_2 = \begin{pmatrix} abcd \\ bacd \end{pmatrix} \quad \pi_3 = \begin{pmatrix} abcd \\ bdac \end{pmatrix}$$

Then

$$(\pi_1 \circ \pi_2) \circ \pi_3 = \begin{pmatrix} abcd \\ dabc \end{pmatrix} \circ \begin{pmatrix} abcd \\ bdac \end{pmatrix} = \begin{pmatrix} abcd \\ acdb \end{pmatrix}$$

$$\pi_1 \circ (\pi_2 \circ \pi_3) = \begin{pmatrix} abcd \\ adbc \end{pmatrix} \circ \begin{pmatrix} abcd \\ adbc \end{pmatrix} = \begin{pmatrix} abcd \\ acdb \end{pmatrix}$$

Permutation Group

Theorem 1:

$(A, \circ)$ is a group

Proof :

1. $\circ$ is both closed and associative
2. There exists an identity permutation, which maps each element into itself
3. The inverse of π is one that maps $\pi(a)$ into a

Permutation Group

Definition : A subgroup $(G, \circ)$ of $(A, \circ)$ is called a permutation subgroup

Ex :

$$G = \left\{ \begin{pmatrix} abcd \\ abcd \end{pmatrix}, \begin{pmatrix} abcd \\ bacd \end{pmatrix}, \begin{pmatrix} abcd \\ abdc \end{pmatrix}, \begin{pmatrix} abcd \\ badc \end{pmatrix} \right\}$$

Permutation Group

Definition :

A binary relation induced by a permutation group $(G, \circ)$ is a relation R such that

an element a is related to b

$\Leftrightarrow$ some permutation in G maps a to b

Ex : In the previous G,

a is related to b, b is related to a

c is related to d, d is related to c

Permutation Group

Theorem 2:

A binary relation *R* induced by a permutation group $(G, \circ)$ is an equivalence relation

Proof :

1. $a\ R\ a$ (due to identity)
2. $a\ R\ b \Rightarrow b\ R\ a$ (due to inverse)
3. $a\ R\ b$ and $b\ R\ c \Rightarrow a\ R\ c$ (due to associative)

Permutation Group

Corollary :

> A binary relation R induced by a permutation group $(G, \circ)$ of S partitions the elements in S

Ex :

The binary relation on the previous G partitions the elements $\{ a, b, c, d \}$ into two equivalence classes : $\{ a, b \}$ and $\{ c, d \}$

Burnside's Theorem

- Let $\psi(\pi)$ denote the number of elements that are invariant under the permutation π

Theorem 3 (Burnside) :

Let R be the equivalence relation induced by a permutation group $(G, \circ)$ of S.

Then # classes that R partitions S into is :

$$\frac{1}{|G|} \sum_{\pi \in G} \psi(\pi)$$

Burnside's Theorem

Ex :

$$G = \left\{ \begin{pmatrix} abcd \\ abcd \end{pmatrix}, \begin{pmatrix} abcd \\ bacd \end{pmatrix}, \begin{pmatrix} abcd \\ abdc \end{pmatrix}, \begin{pmatrix} abcd \\ badc \end{pmatrix} \right\}$$

- Total number of invariant elements

  $= 4 + 2 + 2 + 0 \ = 8$

- # of equivalence classes $= \ 8 / |G| \ = 2$

Burnside's Theorem

Proof :

Let $\eta(s)$ = # permutations that s is invariant

Then we have :

$$\sum_{\pi \in G} \psi(\pi) = \sum_{s \in S} \eta(s)$$

Let a and b be two elements that are in the same equivalence classes

➔ Exactly $\eta(a)$ permutations maps a to b (why?)

Burnside's Theorem

Proof (cont) : The reason is that :

Suppose $J = \{ \pi_1 , \pi_2 , \pi_3 , \pi_4 , \ldots \}$ are all $\eta(a)$ permutations that a is invariant, and π is some permutation that maps a to b (why π exits?)

Then $K = \{ \pi \circ \pi_1 , \pi \circ \pi_2 , \pi \circ \pi_3 , \pi \circ \pi_4 , \ldots \}$ contains $\eta(a)$ permutations that maps a to b

Also, for any π' that maps a to b

$\pi^{-1} \circ \pi'$ is in J, so that $\pi' = \pi \circ \pi^{-1} \circ \pi'$ is in K

➔ Exactly $\eta(a)$ permutations maps a to b

Burnside's Theorem

Proof (cont) :

Now, let $L = \{ a, b, c, d, \ldots, h \}$ be the elements in the same class as a

Because each permutation in G maps a to some element in L ➔ $|L|\,\eta(a) = |G|$

Then we have :

$$|G| / |L| = \eta(a) = \eta(b) = \ldots = \eta(h)$$

or

$$\eta(a) + \eta(b) + \eta(c) + \ldots + \eta(h) = |G|$$

Burnside's Theorem

Proof (cont) :

Thus, for any equivalence class,

sum of $\eta(s)$ for all s in that class = $|G|$

Immediately, we have :

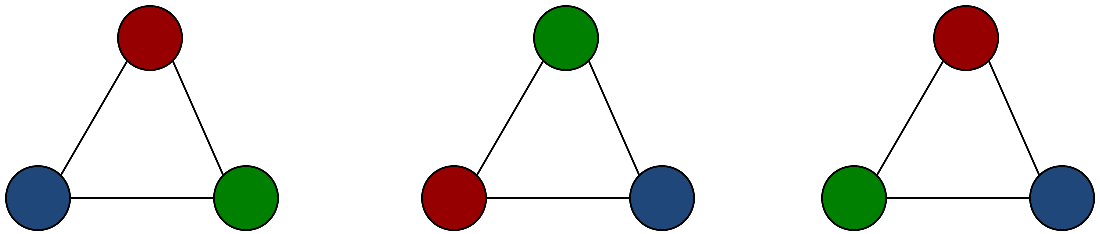
$$\#\text{ equivalence class} = \sum_{s \in S} \eta(s) \ / \ |G|$$

Burnside's Theorem

Ex : Suppose an equilateral triangle has each of its vertices colored by one of the 5 colors

We consider two colorings to be equivalent if after a rotation, they become the same

For instance, first 2 colorings are equivalent, but the third coloring is different from them



Burnside's Theorem

Q : How many distinct colorings are there ?

A : Let S be the set of all 5^3 colorings

Let $(G, \circ)$ be permutation group such that each permutation in G correspond to a possible mapping of a coloring to another due to a series of rotations

➔ G has 3 elements :

Identity, Rotate by 120°, Rotate by 240°

Burnside's Theorem

Answer (cont) :

To find out the number of distinct colorings, it is the same as to find out how many equivalence classes that will be obtained by the relation induced by $(G, \circ)$

➔ Since each class contains a particular set of equivalent colorings

By Burnside, the number of classes is :

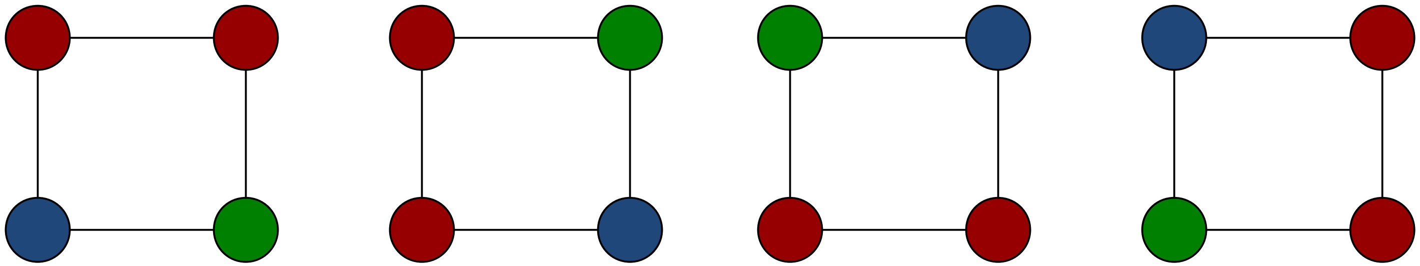
$$(5^3 + 5 + 5) / 3 = 45$$

Burnside's Theorem

Ex : Suppose a square has each of its vertices colored by one of the 7 colors

We consider two colorings to be equivalent if after a rotation, they become the same

How many distinct colorings ?



Burnside's Theorem

Answer :

Let $(G, \circ)$ be a permutation group, such that G contains all the possible permutations obtained by a series of rotations

➔ G has four elements :

Rotate by 0°, by 90°, by 180°, and by 270°

➔ By Burnside, the number of classes is :

$$(7^4 + 7 + 7^2 + 7) / 4 = 616$$

Burnside's Theorem

Ex : Let p = prime.

a = a number coprime to p

Suppose a regular p-gon has each of its vertices colored by one of the a colors

We consider two colorings to be equivalent if after a rotation, they become the same

Q: How many distinct colorings ?

Burnside's Theorem

A : Let G be the p different rotations.

➔ By Burnside, the number of classes is :

$$(a^p + a + a + \ldots + a) / p$$

$$= (a^p + (p - 1)\, a) / p$$

This implies that $a^p - a$ *must be* a multiple of p

➔ $a^p \equiv a \pmod{p}$ or $a^{p-1} \equiv 1 \pmod{p}$

➔ A new proof of Fermat's Little Theorem

Burnside's Theorem

Ex : Let *S* be the set of all 10^5 five-digit number.

Two numbers in *S* are considered equivalent if one can read the other upside down

For example,

99861 and 19866 are equivalent

but 99861 and 66891 are not

Q: How many distinct numbers are there ?

Burnside's Theorem

Answer :

Let $(G, \circ)$ be the permutation group such that G contains all the possible permutations obtained by a sequence of upside-down rotations

➔ G has 2 elements : identity, "upside-down"

where "upside-down" maps :

(i) a number to itself when it is not readable upside-down (e.g., 13567 to 13567)

(ii) otherwise, a number to its equivalent

Burnside's Theorem

Answer (cont) :

By Burnside, the # of equivalence classes is :

$$(10^5 + (10^5 - 5^5) + 3 \times 5^2) / 2 = 98475$$

- Here, $10^5 - 5^5$ counts those numbers that contain at least one 2, 3, 4, 5, or 7
- Here, 3×5^2 counts those numbers formed by only 0, 1, 6, 8, and 9 which are invariant upside-down (must have 0/1/8 at the center)