Applications of Group Theory in Probability and Graph Theory

By:

Prof. Ahmad Erfanian

Department of Pure Mathematics,

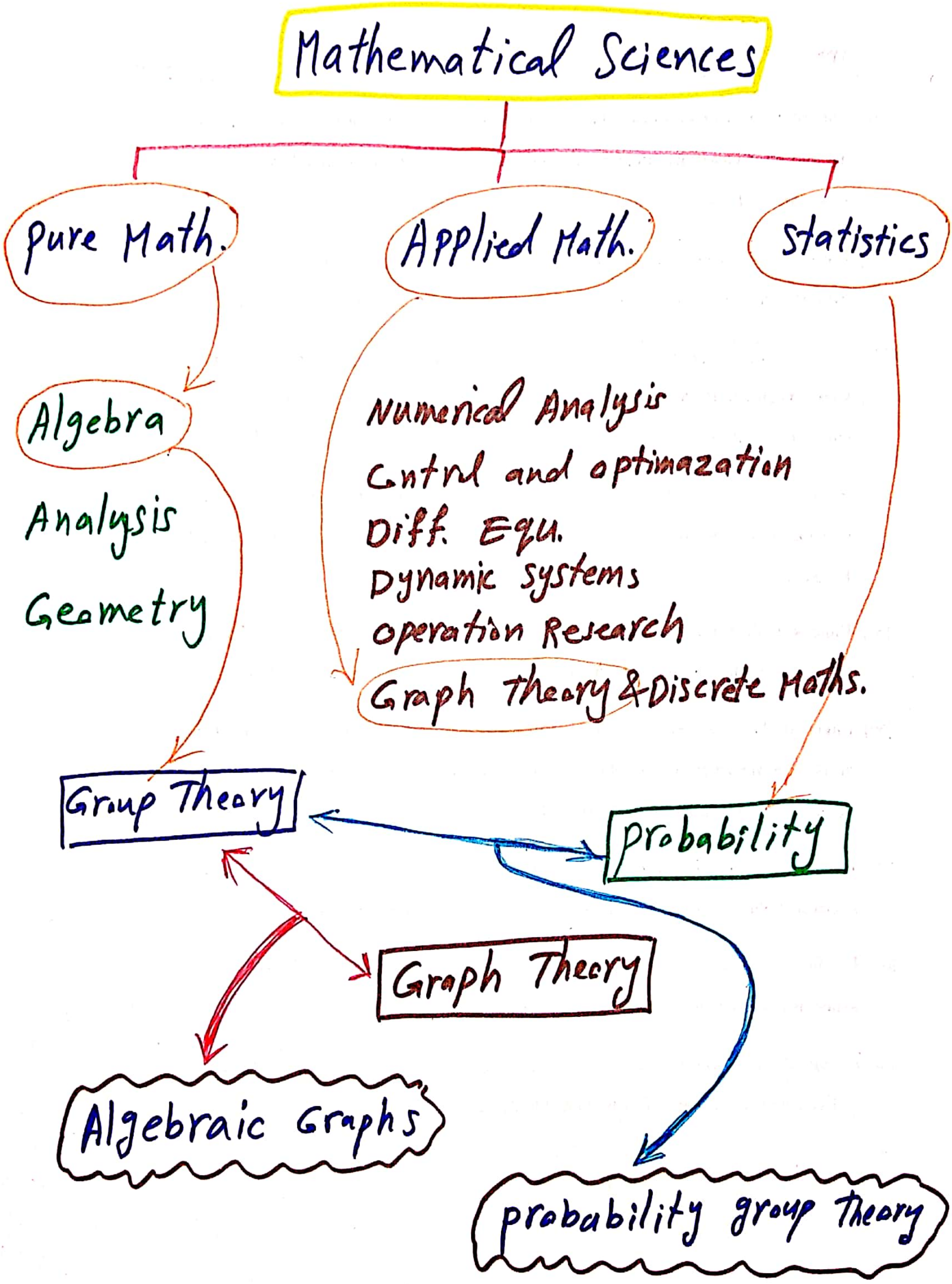
Faculty of Mathematical Sciences, Ferdowsi University of Mashhad, Mashhad, Iran.

Part 1 : Some Probabilities in Group Theory

Monday	18 January, 2021	3.30 p.m. - 5.00 p.m.
Wednesday	20 January, 2021	3.00 p.m. - 5.00 p.m.

Part 2 : Some Graphs Associated to Groups

Monday	25 January, 2021	2.00 p.m. - 4.00 p.m.
Wednesday	27 January, 2021	3.00 p.m. - 5.00 p.m.


Mathematical Sciences
Pure Math.
Applied Math.
Statistics
Algebra
Analysis
Geometry
Numerical Analysis
Cntrl and optimazation
Diff. Equ.
Dynamic systems
operation Research
Graph Theory & Discrete Maths.
Group Theory
probability
Graph Theory
Algebraic Graphs
probability group Theory

Application of Group Theory in Probability Theory

What is the definition of probability?

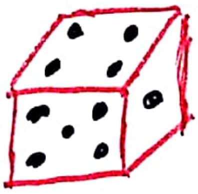
Definition

probability of an event = # of ways it can be happen / total number of outcomes

A = event

$$P(A) = \frac{\#\text{ of ways } A \text{ can happen}}{\text{Total number of autcomes}}$$

Example Dice



A = Having number 1

B = Having numbers 2 or 5

C = Having an odd number

$$P(A) = \frac{1}{6} \; ; \; P(B) = \frac{2}{6} \; ; \; P(C) = \frac{3}{6}$$

Some probabilities in Group Theory

1 Commutativity Degree

Definition Let G be a finite group. Then the commutativity degree of G is the probability of two random elements x and y commute. In other words, the commutativity degree of G, denoted by $d(G)$ is the following ratio:

$$d(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2}$$

Definition A group G is called **abelian** or **commutative**, if all elements of G commute. In other words, for every two arbitrary elements x and y, we have $xy = yx$.

Note $d(G) = 1 \iff G$ is abelian

Proof. If G is abelian, then obviously $d(G) = 1$. Conversely, if $d(G) = 1$, then we have

$|G|^2 = |\{(x,y) \in G \times G \mid xy = yx\}|$. So, we have $xy = yx$ for all $x, y \in G$. Hence G is abelian (Commutative).

Example Let S_3 be symmetric group on 3 symboles. So, $S_3 = \{e, (12), (13), (23), (123), (132)\}$ and we have :

e : e commute with all six elements.

$(e,e), (e,(12)), (e,(13)), (e,(23)), (e,(123)),$
$(e,(132))$ we have 6 pairs

(12) : (12) Commutes with only e and (12).

$((12),e), ((12),(12))$

(13) : (13) Commutes with only e and (13)

$((13),e), ((13),(13))$

(23) : (23) Commutes with only e and (23).

$((23),e), ((23),(23))$

(123) : (123) Commutes with e, (123), (132).

$((123),e), ((123),(123)), ((123),(132))$

(132); (132) commutes with e, (132), (123).

$((132), e)$, $((132), (132))$, $((132), (123))$

Hence, we have:

$$d(S_3) = \frac{|\{(x,y) \in S_3 \times S_3 \mid xy = yx\}|}{|S_3|^2}$$

$$= \frac{|\{(e,e), (e,(12)), (e,(13)), (e,(23)), (e,(123)), (e,(132)),}{6^2}$$

$$\frac{((12),e), ((12),(12)), ((13),e), ((13),(13)), ((23),e), ((23),(23)), ((123),e),}{}$$

$$\frac{((123),(123)), ((123),(132)), ((132),e), ((132),(132)), ((132),(123))\}|}{}$$

$$= \frac{18}{36} = \frac{1}{2} \implies d(S_3) = \frac{1}{2}$$

Example Let D_8 be dihedral group of order 8. Then

$$D_8 = \langle a, b \mid a^4 = b^2 = e,\ bab = a^{-1} \rangle$$
$$= \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

one can easily by a simple computation see that $d(D_8) = \frac{40}{64} = \frac{5}{8}$

Definition Let G be a group. Then the centralizer of element x in G, denoted by $C_G(x)$ is defined as follows:

centralizer of $x = C_G(x) = \{y \in G \mid xy = yx\}$.

Moreover, the centre of G, denoted by $Z(G)$ is:

$$Z(G) = \{x \in G \mid xg = gx \quad \forall g \in G\}$$

Note 1 $Z(G) = G \iff G$ is abelian

Note 2 $Z(G) = \bigcap_{x \in G} C_G(x)$

Note 3 If $x \in Z(G)$, then $C_G(x) = G$.

If $x \notin Z(G)$, then $C_G(x) \lneqq G$.

Thus $|C_G(x)| \leq \frac{|G|}{2}$.

Note 4 If G is not abelian, then

$$\frac{|G|}{|Z(G)|} \geq 4.$$

Lemma $d(G) = \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)|$

proof It is clear that if $G = \{x_1, x_2, \dots, x_n\}$, then

$$|\{(x,y) \in G \times G \mid xy = yx\}| = |\{(x_1, y) \mid \underset{y \in G}{yx_1 = x_1 y}\}| + |\{(x_2, y) \mid \underset{y \in G}{x_2 y = y x_2}\}| + \dots + |\{(x_n, y) \mid \underset{y \in G}{x_n y = y x_n}\}|$$

$$= |C_G(x_1)| + |C_G(x_2)| + \dots + |C_G(x_n)| = \sum_{x \in G} |C_G(x)|$$

and the proof follows.

Lemma Let G be a finite non-abelian group. Then $d(G) \leq \frac{5}{8}$.

proof We have by the above lemma,

$$d(G) = \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)| = \frac{1}{|G|^2} \left(\sum_{x \in Z(G)} |C_G(x)| + \sum_{x \notin Z(G)} |C_G(x)| \right)$$

$$\leq \frac{1}{|G|^2} \left(|Z(G)||G| + (|G| - |Z(G)|) \frac{|G|}{2} \right) = \frac{1}{|G|^2} \left(\frac{|G|^2}{2} + \frac{|Z(G)||G|}{2} \right) = \frac{1}{2} + \frac{1}{2} \frac{|Z(G)|}{|G|} \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1}{4}\right) = \frac{5}{8}$$

Theorem Let G be a finite non-abelian group. Then $d(G)=\frac{5}{8} \iff \frac{G}{Z(G)} \cong Z_2 \times Z_2$.

Theorem Let G be a finite non-abelian group and p be the smallest prime number dividing $|G|$. Then $d(G) \leq \frac{p^2+p-1}{p^3}$.

Theorem Let G be a finite group and H be a subgroup of G. Then

$$\frac{1}{[G:H]^2} d(H) \leq d(G) \leq d(H)$$

Theorem Let G be a finite group and N be a normal subgroup of G. Then

$$d(G) \leq d(N)\, d\left(\frac{G}{N}\right)$$

Theorem Let p be the smallest prime number dividing $|G|$. If $d(G) > \frac{1}{p}$, then G is a nilpotent group of class at most 2.

2 Relative Commutativity Degree

Definition Let G be a finite group and H be a subgroup of G. The **relative commutativity degree of H in G**, denoted by $d(H,G)$ is defined as the following ratio:

$$d(H,G)=\frac{|\{(x,y)\in H\times G \mid xy=yx\}|}{|H||G|}$$

Note If $H=G$, then $d(G,G)=d(G)$.

Example Let $G=S_3=\{e,(12),(13),(23),(123),(132)\}$ and $H=\{e,(12)\}$. Then we have

$$d(H,S_3)=\frac{|\{(e,e),(e,(12)),(e,(13)),(e,(23)),(e,(123)),(e,(132)),((12),e),\ldots((12),(12))\}|}{|H||S_3|}=\frac{8}{2\times 6}=\frac{8}{12}=\frac{2}{3}$$

Similarly, if $\cancel{H}K=\{e,(123),(132)\}$, then

$$d(K,S_3)=\frac{12}{\cancel{2}3\times 6}=\frac{12}{18}=\frac{2}{3}$$

Example Let D_8 be dihedral group of order 8. Then we have

$D_8 = \langle a, b \mid a^4 = b^2 = e,\ bab = a^{-1} \rangle$
$= \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, $Z(D_8) = \{e, a^2\}$

It is clear that $d(Z(D_8), D_8) = 1$. Now for subgroups $H = \{e, b\}$ and $K = \{e, a, a^2, a^3\}$ we can see that

$$H : \begin{cases} e \longrightarrow \text{commutes with all 8 elements} \\ b \longrightarrow \text{commutes with elements } e, b, a^2, a^2b \end{cases}$$

Thus $d(H, D_8) = \dfrac{8+4}{|H||D_8|} = \dfrac{12}{2 \times 8} = \dfrac{3}{4}$

$$K : \begin{cases} e \longrightarrow \text{commutes with 8 elements} \\ a \longrightarrow \text{commutes with } e, a, a^2, a^3 \\ a^2 \longrightarrow \text{commutes with 8 elements} \\ a^3 \longrightarrow \text{commutes with } e, a, a^2, a^3 \end{cases}$$

Thus

$$d(K, D_8) = \frac{8+4+8+4}{|K||D_8|} = \frac{24}{32} = \frac{3}{4}$$

Lemma Let G be a finite group and H be a subgroup of G. Then we know that the centralizer of element $x \in G$ in H is

$$C_H(x) = \{h \in H \mid hx = xh\} \quad (x \in G)$$

Then

$$d(H,G) = \frac{1}{|H||G|} \sum_{x \in G} |C_H(x)|$$

$$= \frac{1}{|H||G|} \sum_{h \in H} |C_G(h)|$$

proof It follows from the point that

$$|\{(h,x) \in H \times G \mid hx = xh\}| = \sum_{x \in G} |C_H(x)|$$

$$= \sum_{h \in H} |C_G(h)|$$

Theorem Let H be a subgroup of G.

Then

$$d(G) \leqslant d(H,G) \leqslant d(H)$$

proof $d(H,G) = \frac{1}{|H||G|} \sum_{x \in G} |C_H(x)|$

$$= \frac{1}{|G|} \sum_{x \in G} \frac{|C_H(x)|}{|H|} \geq \frac{1}{|G|} \sum_{x \in G} \frac{|C_G(x)|}{|G|}$$

$$= \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)| = d(G)$$

Similarly, $d(H,G) = \frac{1}{|H||G|} \sum_{h \in H} |C_G(h)|$

$$= \frac{1}{|H|} \sum_{h \in H} \frac{|C_G(h)|}{|G|} \leq \frac{1}{|H|} \sum_{h \in H} \frac{|C_H(h)|}{|H|}$$

$$= \frac{1}{|H|^2} \sum_{h \in H} |C_H(h)|$$

(Note: $[H : C_H(x)] \leq [G : C_G(x)] \quad \forall x \in G$)

Example $G = S_4$, $H = A_4$

$d(H) = \frac{1}{3}$

$d(H,G) = \frac{1}{4}$ $\qquad \frac{5}{24} < \frac{1}{4} < \frac{1}{3}$

$d(G) = \frac{5}{24}$

Some Results

Theorem Let G be a group and H, N be subgroups of G such that $N \trianglelefteq G$, $N \leq H$. Then $d(H,G) \leq d\left(\frac{H}{N}, \frac{G}{N}\right) d(N)$

Theorem Let G_1 and G_2 be two groups and H_1, H_2 be subgroups of G_1 and G_2, respectively. Then

(i) $d(G_1 \times G_2) = d(G_1)\, d(G_2)$

(ii) $d(H_1 \times H_2) = d(H_1)\, d(H_2)$

(iii) $d(H_1 \times H_2, G_1 \times G_2) = d(H_1, G_1)\, d(H_2, G_2)$

Theorem Let G be non-abelian group and p be the smallest prime number dividing $|G|$. Then

(i) If $H \subseteq Z(G)$, then $d(H,G) = 1$.

(ii) If $H \nsubseteq Z(G)$ and H abelian, then

$$d(H,G) \leq \frac{2p-1}{p^2}$$

(iii) If $H \nsubseteq Z(G)$ and H non-abelian, then

$$d(H,G) \leq \frac{p^2+p-1}{p^3}$$

Theorem Let G be a group and H be a subgroup of G. If p is the smallest prime number divide $|G|$. Then

(i)

$$\frac{|Z(G)\cap H|}{|H|} + p\frac{(|H|-|Z(G)\cap H|)}{|H||G|} \leq d(H,G)$$

$$\leq \frac{(p-1)|Z(G)\cap H| + |H|}{p|H|}$$

(ii) $$d(H,G) \leq \frac{1}{p}\left(1+(p-1)\frac{|Z(G)\cup Z(H)|}{|G|}\right)$$

Theorem Let G be a group and H be a subgroup of G. Then

(i) If $d(H,G)=\frac{3}{4}$, then $\frac{H}{Z(G)\cap H} \cong Z_2$

(ii) If $d(H,G)=\frac{5}{8}$ and H non-abelian then

$$\frac{H}{Z(G)\cap H} \cong Z_2 \times Z_2$$

Exercises

1. Let G be a finite group and H be a subgroup of G. If $G = HC_G(x)$ for all $x \in G$, then prove that $d(G) = d(H, G)$.

2. Let D_{2n} be dihedral group of order $2n$. Then find $d(D_{2n})$?

3. Let G be a finite group and H_1, H_2 ~~are~~ be subgroups of G such that $H_1 \leq H_2$. Then prove that
$$d(H_2, G) \leq d(H_1, G) \leq d(H_1, H_2)$$

4. Let G be a finite group and $K(G)$ be the number of conjugacy classes of G. Then prove that $d(G) = \frac{K(G)}{|G|}$.