**COSETS, Recap**

\[ H \trianglelefteq G \]

\[ \{h_1, \ldots, h_n\} \]

\[ x \sim y \iff xy^{-1} \in H \]

**Equivalence Classes:**

\[ Hz = \{h_1z, h_2z, \ldots, h_nz\} \] is a coset

**What do we know about coset \( Hz \)?**

- \( z \in Hz \)
- \( z' \in Hz \implies Hz' = Hz \)
- \( z' \notin Hz \implies Hz' \cap Hz = \emptyset \)

**Cosets**

\[ Hze, Hz_1, Hz_2, \ldots, Hz_n \]
A FURTHER EXAMPLE

\[ G = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} = \mathbb{Z} \]
\[ H = \{ \ldots, -10, -5, 0, 5, 10, \ldots \} = 5\mathbb{Z} \]

**NOTE:** \( H+1 = H+6 = H-4 = \ldots \)

ETC.
LAGRANGE THEOREM

IF $G$ IS FINITE AND $H \leq G$ THEN $|H|$ DIVIDES $|G|$

PROOF: $G = H \cup H_2 \cup H_2 \cup \ldots$

CLAIM: $|HZ| = |H|$

PROOF: $HZ = \{h_i z, h_2 z, \ldots \}$

\[ h_i z = h_j z \iff h_i = h_j \]

\[ (h_i z z^{-1} = h_j z z^{-1} \rightarrow h_i = h_j) \]

Q.E.D.

DEFINITION [INDEX]: $|G|/|H|$

INDEX OF $H$ IN $G$
LAGRANGE'S THEOREM IN PICTURES

All cosets have the same size, so $|H| |G|$

$H = \{ h_1, h_2, h_3, \ldots, h_m \}$

$H^z = \{ h_1^z, h_2^z, h_3^z, \ldots, h_m^z \}$

1-1 Map
LEMMA: Let G be a finite group. Then G has a generator set \( \Gamma \) s.t. 
\[ \left| \Gamma \right| \leq \log_2 |G| \]

PROOF: Pick any \( g_i \in G \) s.t. \( g_i \neq e \)

If \( g_1, g_2, \ldots, g_i \) are already picked

Pick \( g_{i+1} \not\in \langle g_1, \ldots, g_i \rangle = G_i \)

CLAIM: \( |G_i| / |G_{i-1}| \geq 2 \)

PROOF: \( G_{i-1} < G_i \). Apply Lagrange Thm.

\[ \Rightarrow |G_{i-1}| \text{ is an integer multiple of } |G_{i-1}|, \neq 1 \]

In \( \leq \log_2 |G| \) step procedure

Stops with \( G_i = G \)
$\exists \log |G| \text{ SIZE GENERATOR SET (RECAP)}$

$\frac{|H_i|}{|H_{i-1}|} \geq 2$
PERMUTATION GROUPS

PERMUTATIONS OF \( A = 1-1 \) MAPS \( A \to A \)

NOTATION:
\[
\pi = \left( a_1, a_2, ..., a_n \right) \quad A = \{a_1, a_2, ..., a_n\}
\]

\( a_{\pi(i)} = a_{\pi(j)} \) FOR \( i \neq j \)

EXAMPLE: \( A = \{1, 2, 3\} \)

\[
\pi: \begin{array}{c}
  1 \rightarrow 1 \\
  2 \rightarrow 2 \\
  3 \rightarrow 3 \\
\end{array}
\]

\( \pi = (1 \ 3 \ 2) \)

CYCLE STRUCTURE:
(1)(23)

IN GENERAL

\[
\pi = (a, a_{\pi(i)}, a_{\pi(\pi(i))}, ...) (\ldots) (\ldots)
\]

ORDER OF CLAUSES DOES NOT MATTER
PERMUTATION GROUPS, CONTINUED

MULTIPLICATION:

\[ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} \]

\[ \sigma \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}, \quad \pi \rightarrow 2 \sigma \rightarrow 4 \]

\[ \sigma \cdot \pi (i) = \sigma(\pi(i)) \]

COMPOSITION OF BIJECTIONS IS A BIJECTION

INVERSE:

\[ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}, \quad \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 3 & 5 \end{pmatrix} \]

\[ \pi (i) = j \iff \pi^{-1} (j) = i \]

\[ S_A = \text{GROUP OF ALL PERMUTATIONS ON A} \]

\[ S_n = \text{GROUP OF ALL PERMUTATIONS ON } \{1, 2, \ldots, n\} \]
PERMUTATION GROUPS, CONTINUED

**Definition:** $G$ is a permutation group if it is a group represented as a set of permutations on $A$. ($G \leq S_A$)

**Warning:** The same group may have more than one permutation representations:

\[ S_3 = \{ (1 2 3), (1 3 2), (2 1 3), (2 3 1), (3 1 2), (3 2 1) \} \]

\[
\begin{array}{c|cccc}
  & e & r & r^2 & f_1, f_2, f_3 \\
\hline
  e & e & r & r^2 & f_1, f_2, f_3 \\
r & r & r^2 & f_2, f_3 & f_1 \\
r^2 & r^2 & f_2, f_3 & f_1 & f_2 \\
f_1 & f_1 & f_3 & f_2 & e \\
f_2 & f_2 & f_3 & f_1 & r \\
f_3 & f_3 & f_2 & f_1 & r^2 \\
\end{array}
\]

\[
\begin{array}{c}
  (1 2 3), (1 3 2), (2 1 3), (2 3 1), (3 1 2), (3 2 1) \\
  e, r, r^2, f_1, f_2, f_3 \\
\end{array}
\]

Different permutation representation of $S_3$.
TWO DIFFERENT PERMUTATION REPRESENTATIONS OF $S_4$

$S_4$ ON VERTICES

$S_4$ ON EDGES

\{1,2\} \{1,3\} \{1,4\} \{2,3\} \{2,4\} \{3,4\}

\{1,2\} \{1,3\} \{1,4\} \{2,3\} \{2,4\} \{3,4\}
THE GRAPH ISOMORPHISM PROBLEM

**Definition:** Graphs $X_1$ and $X_2$ are isomorphic if there is a 1-1 map $\pi: V(X_1) \rightarrow V(X_2)$ that takes edges into edges and non-edges into non-edges.

**Graph-ISO:** Given $X_1, X_2$, find out if they are isomorphic.

Recent: Graph-ISO $\in$ \text{TIME}(n^{(\log n)^{O(1)}})$

László Babai
THE GRAPH AUTOMORPHISM PROBLEM

GRAPH-AUT: Given a graph $X$ find a generator set for

$$\text{AUT}(X) \leq S_{V(X)}$$

NOTE: $\text{AUT}(X)$ may be exponentially large, but always has a
set $\Gamma'$ of generators where

$$|\Gamma'| \leq \log_2 n! \sim n \log n$$

$n \overset{\text{def}}{=} |V(X)|$

$X = K_n$

$\text{AUT}(K_n) = S_n$

$\Gamma' = \text{set of all transpositions}$

$|\Gamma'| = (n)$
COLOR AUTOMORPHISM PROBLEM

COLOR-AUT: \text{INPUT} = \text{COLORED SET} ~ A
\Gamma \leq S_A

\text{OUTPUT} = \text{GENERATORS FOR THE SUBGROUP OF} ~ \langle \Gamma \rangle
\text{OF THE COLOR PRESERVING MAPS}

COLOR PRESERVING PERMUTATION:

\pi, \pi^0 \text{ ARE COLOR PRESERVING}
\pi \pi^0 \text{ IS ALSO}
\pi^{-1} \text{ IS ALSO}
POLY TIME REDUCTION

GRAPH-AUT $\rightarrow$ COLOR-AUT

INPUT

\[
\begin{array}{c}
1 \\
3 \\
4 \\
2
\end{array}
\]

\[
\begin{array}{c}
1 \\
2 \\
3 \\
4
\end{array}
\]

INPUT

\[
\text{COLORED SET} = \{1, 2, 3, \ldots, 3, 4\}^2
\]

\[
\text{GROUP} = S_4 \text{-ON-EDGES}
\]

AUTOMORPHISM IFF PRESERVES COLORS

\[
\begin{array}{c}
1 \\
2 \\
3 \\
4
\end{array} \overset{\text{AUT}}{\rightarrow} \begin{array}{c}
1 \\
3 \\
4 \\
2
\end{array}
\]

\[
\begin{array}{c}
1 \\
3 \\
4 \\
2
\end{array} \not\overset{\text{NOT-AUT}}{\rightarrow} \begin{array}{c}
1 \\
3 \\
4 \\
2
\end{array}
\]
**Lemma:** Graph-iso reduces to Graph-out

**Proof:**

W.l.o.g. assume that $X_1, X_2$ are connected.

Determine $\text{Aut}(X_1 \cup X_2)$.

$\Gamma =$ generator set for $\text{Aut}(X_1 \cup X_2)$.

If any $g \in \Gamma$ swaps $X_1$ and $X_2$, then $X_1 \cong X_2$, otherwise $X_1 \not\cong X_2$.
WE HAVE RELIED ON:

IF \( G = \langle g_1, g_2, \ldots \rangle \) AND ALL \( g_i \) RESPECT

\[
\begin{array}{c|c}
\text{LEFT} & \text{RIGHT} \\
1 & 5 \\
2 & 6 \\
3 & 7 \\
4 & 8 \\
\end{array}
\]

\( g_1 \)

\( g_2 \)

\vdots

THEN ALL ELEMENTS OF \( G \) WILL RESPECT LEFT \| RIGHT

\[ g = g_1^{-1} g_2 g_3 g_4 \ldots \]

DO NOT MIX LEFT–RIGHT
WE HAVE ALSO RELIED ON

\[ X = X_1 \cup X_2 \]

IS AN AUTOMORPHISM MADE FROM
AND ALSO

1. IF \( \pi \in \text{AUT}(X, \cup X_2) \) AND \( v, \pi(v) \in X_2 \) THEN \( \pi(X_2) = X_2 \)

SO, UNDER IT SIDES MUST ALTERNATE

BUT: CAN WE RECOVER AN ISOMORPHISM FROM THIS? NOT ONLY ONE, BUT TWO!!

\[ (x,w) \in E(X_2) \]
\[ \pi(v), \pi(w) \in E(X_2) \]
\[ \pi(w) \in X_2 \]
ALGORITHMS FOR PERMUTATION GROUPS

$G \leq S_n$, given by a set $\Gamma$ of generators

$|G|$ can be large (up to $n!$), $|\Gamma| = n^{O(1)}$

- Determine properties of $G$ (abelian, etc.)
- Size of $G$
- Is $\pi \in G$ (input: $G \leq S_n$, $\pi \in S_n$)
- Compute sub-group of $G$ that respects certain structures
  - For $G_1, G_2$, determine $G_1 \cap G_2$

If answer is group, output is a set of generators
NOTIONS

STABILIZER SUBGROUP

\[ G \leq S_n, \quad i \in \{1, \ldots, n^2\} \]
\[ G_i = \{ \pi \in G \mid i \text{ does not move under } \pi \} \]
\[ G_{i, i_2, \ldots, i_k} = \{ \pi \in G \mid \text{none of } i_1, \ldots, i_k \text{ moves under } \pi \} \]

\[ G \leq S_n, \quad T = \{1, \ldots, n^2\} \]
\[ G_T = \{ \pi \in G \mid \pi \text{ respects } T, T \} \]
GLOBAL STABILIZER OF T

OBSERVATION: LET \( T = \{t_1, t_2, \ldots, t_{n^2}\} \) THEN

\[ G_{t_1, \ldots, t_k} \leq G_T \]

\[ G_{t_1, \ldots, t_k} \overset{\text{def}}{=} G_{\{T\}} \]
POINT-WISE STABILISER OF T
CANONICAL GENERATOR SET FOR G

CONSIDER THE TOWER

\( \{ e \} = G \leq G_{i_3 \cdots n_1} \leq G_{i_1 i_2 \cdots n_2} \leq \cdots \leq G_{i_1} \leq G \)

NOTATION: \( H \leq G, \quad \{ Hz | z \in G \} = G : H \)

NOTATION: \( \{ Z_{i_1}, Z_{i_2}, \ldots, Z_{i_{1 \cdot n_1}} \} = \text{REPR}(G : H) \)

IF IT CONTAINS EXACTLY ONE REPRESENTATIVE FROM EVERY COSET

LET

\( C_1 = \text{REPR}(G : G_i) \)

\( C_{n-1} = \text{REPR}(G_{i_1 i_2 \cdots n_2} : G_{i_1 i_2 \cdots n_1}) \)

CANONCAL GENERATOR SET =

\( C_1 \cup C_2 \cup \cdots \cup C_{n-1} \)
PROPOSITION: CANONICAL GENERATOR SET IS A GENERATOR SET FOR G.

LEMMA: LET \( H \leq G \), \( \Gamma \) BE A GENERATOR SET FOR H. THEN
\[ \Gamma \cup \text{REPR}(G:H) \]
IS A GENERATOR SET FOR G.

PROOF: EVERY \( x \in G \) IS IN SOME \( HZ \)
WHERE \( z \in \text{REPR}(G:H) \). SO \( x = h_{*}z \).
ALSO, \( h = g_{1}^{ \pm 1 } \cdots g_{k}^{ \pm 1 } \) WHERE \( g_{1}, \ldots, g_{k} \in \Gamma \).

PROOF OF THE PROPOSITION IS BY INDUCTION:

ASSUME WE ALREADY KNOW THAT
\[ C_{n-1} \cup C_{n-2} \cup \ldots \cup C_{n-i+1} \]
is a gen. of \( G_{1,2,\ldots,i} \)
THEN
\[ C_{n-1} \cup C_{n-2} \cup \ldots \cup C_{n-i} \]
is a gen. of \( G_{1,2,\ldots,i-1} \)
\[ \text{REPR}(G_{1,2,\ldots,i} : G_{1,2,\ldots,i-1}) \]
CLAIM: \(|G_1 \cup G_2 \cup \ldots \cup G_{n-1}| \leq n(n-1)\)

**Lemma:** \(G \leq S_n\). Then \(|G:G_i| \leq n\)

Let \(O_i = \{1, \ldots, n^2\}\) be the set of all elements where \(G\) can move \(i\) (orbit of \(i\)).

CLAIM 2: \(|G:G_i| = |O_i| (\leq n)\)

Let \(j\) be such that \(\pi(i) = j\) for \(\pi \in G\) then \(\pi G_i = \{g \mid g(i) = j^2\}\)

- \(\forall g \in G_i, g(i) = (\pi h)(i) = j\), where \(h \in O_i\)
- If \(g(i) = j\) then \((\pi^{-1} g)(i) = i\)

So the \(\{g \mid g(i) = j^2\}\) is a left coset of \(G_i\) in \(G\).

\[# of left cosets = |O_i| = |G|/|G_i|\]

\[# of right cosets\]

Original claim trivially follows from lemma.