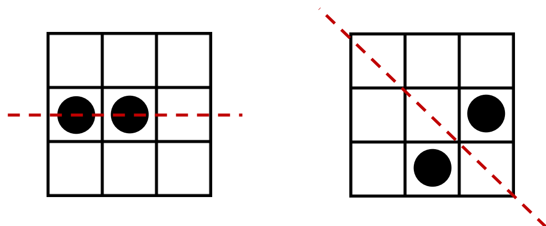
Ma/CS 6a

Class 21: Counting with Permutations



By Adam Sheffer

Repeating the Basics

- We have a set of numbers $X = \{1,2,3,\ldots,n\}$ and a permutation group G of X.
- For example,
$$X = \{1,2,3,4,5,6\}$$
$$G = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

Equivalence Classes

- The group G partitions X into equivalence classes.
  - Two elements $x, y \in X$ are in the same class iff there exists a permutation $g \in G$ such that $g(x) = y$.

$$X = \{1,2,3,4,5,6\}$$
$$G = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

- The classes in this case are $\{1,2\}, \{3,4\}, \{5\}, \{6\}$.

Orbits

- The equivalence classes are also called ***orbits***.
  - For every $x \in X$ the orbit of x is

$$Gx = \{\text{The equivalence class that contains } x\}$$
$$= \{y \in X \mid g(x) = y \ \text{ for some } \ g \in G\}.$$

Another Example: Orbits

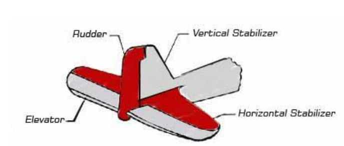
- Let $X = \{1,2,3,4\}$ and let
$G = \{\text{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2),$
$(2\ 4), (1\ 3), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}.$
- What are the orbits/equivalence classes that G induces on X?
  - There is a single class
  $G1 = G2 = G3 = G4 = \{1,2,3,4\}.$

Stabilizers

- The ***stabilizer*** of $x \in X$ is the set of all permutations that take x to itself (x is "stable" in them). We denote this set as G_x.
- Example.

$$X = \{1,2,3,4,5,6\}$$
$$G = \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

- $G_1 = \{id, (3\ 4)\}$.



Example: Stabilizer

- Consider the following permutation group of $\{1,2,3,4\}$:

$$G = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2),\\ (2\ 4), (1\ 3), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}.$$

- The stabilizers are
  - $G_1 = \{\mathrm{id}, (2\ 4)\}$.
  - $G_2 = \{\mathrm{id}, (1\ 3)\}$.
  - $G_3 = \{\mathrm{id}, (2\ 4)\}$.
  - $G_4 = \{\mathrm{id}, (1\ 3)\}$.

Stabilizers are Subgroups

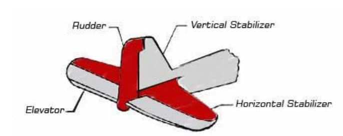
- **Claim.** G_x is a subgroup of G.
  - **Closure.** If $g, h \in G_x$ then $g(x) = x$ and $h(x) = x$. Since $gh(x) = x$ we have $gh \in G_x$.
  - **Associativity.** Implied by the associativity of G.
  - **Identity.** Since $\mathrm{id}(x) = x$, we have $\mathrm{id} \in G_x$.
  - **Inverse.** If $g \in G_x$ then $g(x) = x$. This implies that $g^{-1}(x) = x$ so $g^{-1} \in G_x$.

Recall: Sizes of Orbits and Stabilizers

- **Theorem.** Let G be a group of permutations of the set X. For every $x \in X$ we have

$$|Gx| \cdot |G_x| = |G|.$$

The orbit of x *The stabilizer of x*



Example: Orbits and Stabilizers

- Consider the following permutation group of $\{1,2,3,4\}$:

$$G = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 3), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}.$$

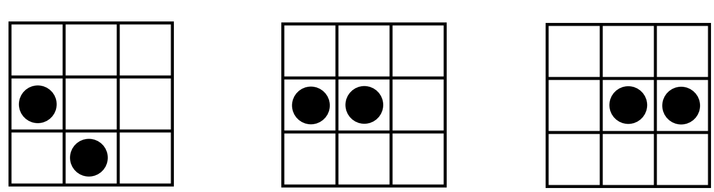
  - We have $|G| = 8$.
  - We have the orbit $G1 = \{1,2,3,4\}$. So $|G1| = 4$.
  - We have the stabilizer $G_1 = \{\mathrm{id}, (2\ 4)\}$. So $|G_1| = 2$.
  - Combining the above yields
$$|G| = 8 = |G1| \cdot |G_1|.$$

Warm-up Problem

- **Problem.** Consider a group of permutations G of the set X. Prove that if $x, y \in X$ are in the same orbit, then $|G_x| = |G_y|$.
- **Proof.**
  - By the assumption, we have $|Gx| = |Gy|$.
  - By the previous theorem
$$|G_x| = \frac{|G|}{|Gx|} = \frac{|G|}{|Gy|} = |G_y|.$$

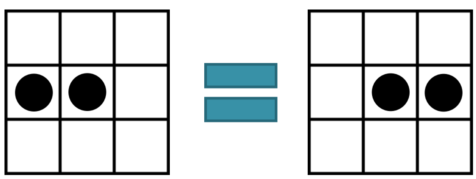
Distinct Identity Cards

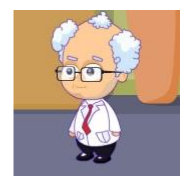
- **(Silly) Problem.** A company produces identity cards that are 3×3 grids with holes in exactly two of the squares.
- How many distinct cards can be produced?
$$\binom{9}{2} = 36.$$



Distinct Identity Cards 2

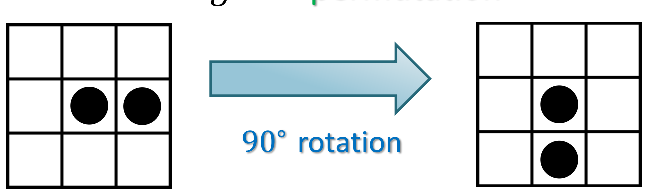
- **Problem (part 2).** The identity cards are given to mathematicians, which might wear them upside down, sideways, back to front, etc.
- How many distinct cards can produced, without a chance of confusing two?





Rephrasing the Problem

- Let X be the set of the original 36 cards.
- Let G be the group of symmetries of a card (combinations of rotations and reflections taking the 3×3 grid to itself).
- Consider a symmetry $g \in G$.
  - Notice that g is a bijection from X to itself.
  - We think of g as a permutation of the set X.



Rephrasing the Problem (2)

- Let X be the set of the original 36 cards.
- Let G be the group of symmetries of a card.
- We think of G is a group of permutations of X.
- The number of distinct cards under the new definition is ***the number of different orbits*** of G on X.
  - We would like a simple way for computing the number of orbits.

Number of Fixed Elements

- For every $g \in G$, we define
$$F(g) = |\{x \in X : g(x) = x\}|.$$
  - $F(g)$ is the number of stabilizers that contain g.
- **Example.** Consider the following permutation group of $\{1,2,3,4\}$.

$$G = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 3), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}.$$

  - $F(\mathrm{id}) = 4.$
  - $F\big((1\ 3)\big) = 2.$
  - $F\big((1\ 2)(3\ 4)\big) = 0.$

The Number of Distinct Orbits

- **Claim.** Let G be a group of permutations of the set X. The number of orbits of G on X is
$$\frac{1}{|G|}\sum_{g\in G}|F(g)|.$$

(= the average size of $F(g)$)

Proof by Double Counting

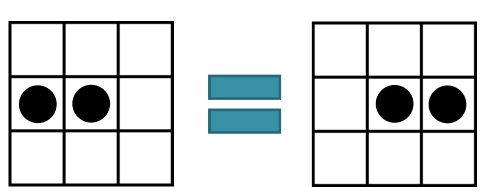
- We ***double count*** the size of the set $E = \{(g,x) \mid g \in G, x \in X, g(x) = x\}$.
- For a fixed $g \in G$, the number of pairs in E that contain g is $F(g)$. That is
$$|E| = \sum_{g\in G} F(g).$$
- For a fixed $x \in X$, the number of pairs that contain x is $|G_x|$. That is,
$$|E| = \sum_{x\in X} |G_x|.$$

Proof (cont.)

- The double counting implies
$$\sum_{g\in G}|F(g)| = \sum_{x\in X}|G_x|.$$
  - Recall that if $x, y \in X$ are in the same orbit, then $|G_x| = |G_y|$.
  - An orbit Gx corresponds to $|Gx|$ elements of the red sum, each of size $|G_x|$. Thus, the orbit contributes to the sum $|Gx||G_x| = |G|$.
  - If there are t orbits then
$$\sum_{g\in G}|F(g)| = t|G| \quad \Rightarrow \quad t = \frac{\sum_{g\in G}|F(g)|}{|G|}.$$

Back to Identity Cards

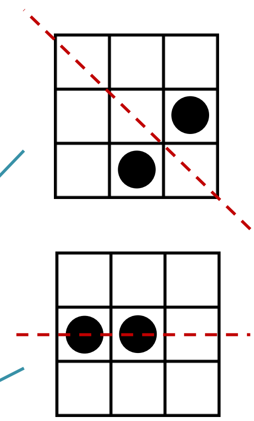
- **Recall.** In the identity cards problem we have a set X of 36 cards. The number of *distinct* cards is the number of orbits under the group G of card symmetries.
  - That is, we need to calculate
$$\frac{\sum_{g\in G}|F(g)|}{|G|}.$$



Counting $|G|$ and $|F(g)|$

- Symmetries of the square and the number of elements that they fix:

Symmetry g	$F(g)$
Identity	36
Rotation 90°	0
Rotation 180°	4
Rotation 270°	0
Reflection: main diagonal	6
Reflection: other diagonal	6
Reflection: vertical bisector	6
Reflection: horizontal bisector	6

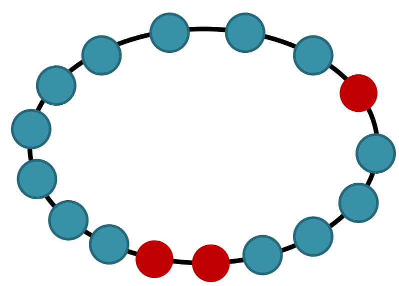


More Counting

- There are eight symmetries of a card, so $|G| = 8$.
- We have
$$\sum_{g \in G} F(g) = 36 + 0 + 4 + 0 + 6 + 6 + 6 + 6.$$
- Therefore, the number of distinct cards/orbits is $\frac{1}{8} \cdot 64 = 8$.

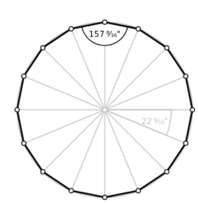
Necklaces

- **Problem.** Necklaces are manufactured by arranging 13 blue beads and three red beads on a loop of string. How many such distinct necklaces are there?



Necklaces Solution

- Think of the necklace as a regular 16-gon.
  - The number of general configurations is $\binom{16}{3} = 560.$
  - Two necklaces are identical if their 16-gons are identical under rotations and reflections (that is, under a symmetry).
  - The number of distinct necklaces is the number of orbits under the symmetry group of the 16-gon.



Necklaces Solution (cont.)

- To count distinct necklaces, we count the number of symmetries and the number of elements fixed by each symmetry.
- For example:
  - The identity symmetry fixes all 560 elements.
  - There are 15 rotations of angles $\frac{2\pi n}{16}$ where $1 \leq n \leq 15$. These do not fix any elements.
- The number of distinct necklaces/orbits is

$$\frac{\sum_g |F(g)|}{|G|} = \frac{672}{32} = 21.$$

Everything is a Permutation Group!

- **Theorem (Cayley).** Every finite group G is isomorphic to a permutation group G'.
- **Proof.**
  - As a set of objects, we take $X = G$.
  - For every $a \in G$, we consider $\pi_a(x) = ax$. This is a *permutation* of $X = G$ due to the *Latin square property* of G.
  - We set $G' = \{\pi_a \mid a \in G\}$ and claim that it is a group.

Example

- Let G be the group $\mathbb{Z}_4 = \{0,1,2,3\}$ under addition $mod\ 4$.
- What is X?
  - $X = \{0,1,2,3\}$.
- What is G'?
  - The set of bijections $\pi_a(x) = a + x\ mod\ 4$.
- For example, π_2 is the permutation

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 0 & 1 \end{array}$$

G' is a Group

- For every $a \in G$, we consider $\pi_a(x) = ax$.
- We set $X = G$ and $G' = \{\pi_a \mid a \in G\}$.
  - **Closure.** We have $\pi_a \pi_b = \pi_c$ where $ab = c \in G$. Thus $\pi_c \in G'$.
  - **Associativity.** We have $(\pi_a \pi_b)\pi_c = \pi_a(\pi_b \pi_c)$ since $(ab)c = a(bc)$ in G.
  - **Identity.** If 1 is the identity of G then π_1 is the identity of G'.
  - **Inverse.** The inverse of π_a is $\pi_{a^{-1}}$, where a^{-1} is the inverse of a in G.

Completing the Proof

- It remains to prove that G and G' are isomorphic.
- We consider the isomorphism β such that for every $a \in G$, we have $\beta(a) = \pi_a$.
- This is an isomorphism since for every $a, b \in G$, we have
  $$\beta(ab) = \pi_{ab} = \pi_a \pi_b = \beta(a)\beta(b).$$

Example: Isomorphic Permutation Group

- Consider the group $G = \{1, -1, i, -i\}$ under standard product.
  - Our set of objects is $X = \{1, -1, i, -i\}$.
  - The permutation group over X is
    $$G' = \{\pi_1, \pi_{-1}, \pi_i, \pi_{-i}\}.$$
  - We have $\pi_1 = \mathrm{id}$.
  - $\pi_i(1) = i, \pi_i(-1) = -i, \pi_i(i) = -1,$ $\pi_i(-i) = 1.$
  - In cycle notation, $\pi_i = (1\ i\ \ -1\ \ -i)$.

The End: A Silly Joke

Why did the algorithmist die in the shower?

Because the shampoo said: