Using symmetry for enumeration

Cheryl E Praeger

Semester 1, 2004

Multiplying Permutations

Let $X = \{1, 2, 3, 4, 5\}$. Following Cameron, I use $g, h, \ldots$ for permutations.

$g = (123)(45)$	$1 \to 2 \to 3 \to 1, \quad 4 \leftrightarrow 5$ so $1g = 2, 2g = 3$ etc
$h = (1)(2345)$ or (2345)	$1 \to 1, \quad 2 \to 3 \to 4 \to 5 \to 2$

To compute $g \circ h$: do g first and then h.

$g \circ h$: $\quad 1 \leftrightarrow 3, \quad 2 \leftrightarrow 4, \quad 5 \to 5$

Hence $g \circ h = \big((123)(45)\big) \circ \big((2345)\big) = (13)(24)$.

We usually write $g \circ h$ as gh.

Symmetric group on $X = \{1, 2, \ldots, n\}$

$\mathrm{Sym}(X) = S_n$ is the group of all permutations of X under composition.

- identity written 1 or 1_X is $(1)(2)\ldots(n)$
- inverses $g \circ g^{-1} = 1$
  For a cycle just reverse the order: $(1234)^{-1} = (4321)$.
  Do this to each cycle for general permutations in cycle notation. Note our convention is to write (4321) as (1432).
  $\big((123)(4897)\big)^{-1} = (321)(7984) = (132)(4798)$
  Warning: in general $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$

Permutation group on X is a subgroup G of $\mathrm{Sym}(X)$.
Just a subset closed under composition: $g, h \in G \Rightarrow \ g \circ h \in G$

Some examples

Take $X = \{1, 2, \ldots, n\}$.

$\mathrm{Sym}(X)$ is the largest permutation group on X: $\quad |\mathrm{Sym}(X)| = n!$

Some examples

Take $X = \{1, 2, \ldots, n\}$.

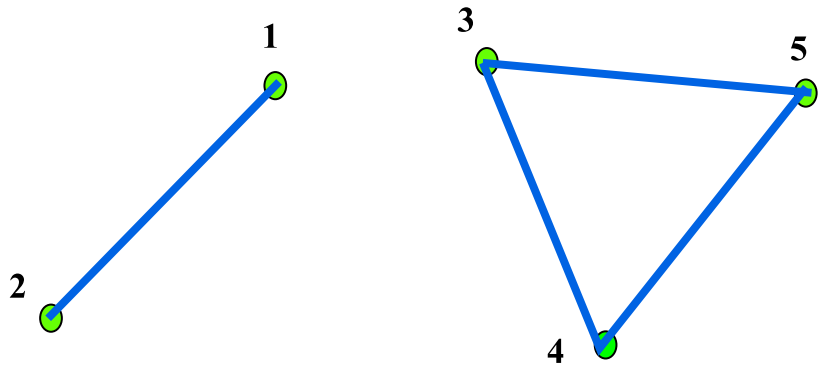
$\mathrm{Sym}(X)$ is the largest permutation group on X: $|\mathrm{Sym}(X)| = n!$

Some smaller examples: $\{1, (12)\}$ $\{1, (345), (354)\}$

Examples: cont

Take $X = \{1, 2, 3, 4, 5\}$.

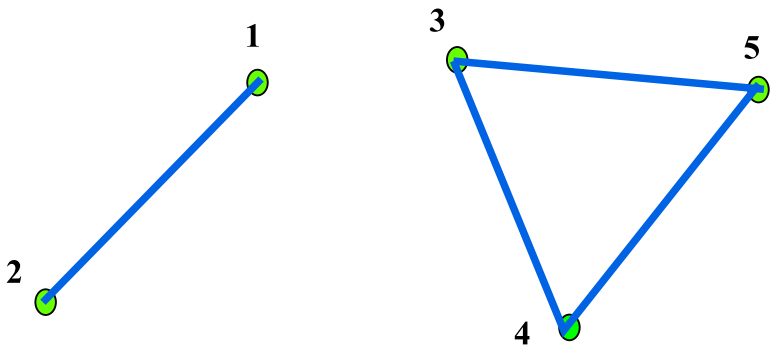
So X is the vertex set
of a graph with edge set



$$E = \{\{1, 2\}, \{3, 4\}, \{4, 5\}, \{3, 5\}\}.$$

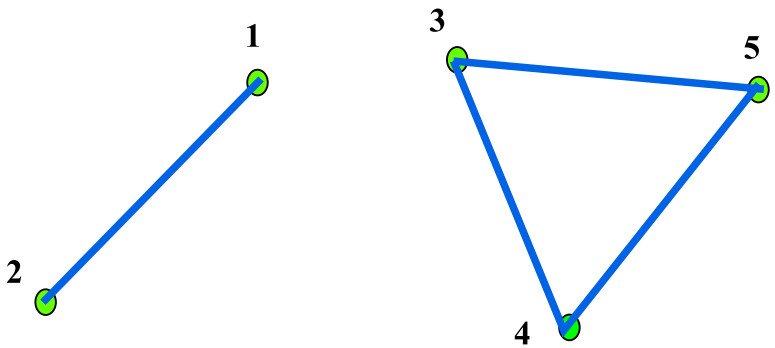
Try to spot some automorphisms of the graph (edge-preserving permutations of the vertices).

Let $G = \langle (12), (345) \rangle$.
(group given by generators)



Then $G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Let $G = \langle (12), (345) \rangle$.
(group given by generators)



Then $G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

We often get permutation groups arising like this in combinatorics.

Can you spot any other automorphisms? If so add them as extra generators. GAP can be used to find the full automorphism group.

Orbits and Stabilisers

$X = \{1, 2, 3, 4, 5\}$ and
$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Orbit of $G \leq \mathrm{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

Orbits and Stabilisers

$X = \{1, 2, 3, 4, 5\}$ and
$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Orbit of $G \leq \mathrm{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$1^G = 2^G = \{1, 2\}$ and $3^G = 4^G = 5^G = \{3, 4, 5\}$.

Orbits and Stabilisers

$X = \{1, 2, 3, 4, 5\}$ and
$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Orbit of $G \leq \mathrm{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$1^G = 2^G = \{1, 2\}$ and $3^G = 4^G = 5^G = \{3, 4, 5\}$.

Stabiliser in G of i is $G_i = \{g \in G \,|\, ig = i\}$.

G_i is a subgroup of G (why?)

Orbits and Stabilisers

$X = \{1, 2, 3, 4, 5\}$ and
$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Orbit of $G \leq \mathrm{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$1^G = 2^G = \{1, 2\}$ and $3^G = 4^G = 5^G = \{3, 4, 5\}$.

Stabiliser in G of i is $G_i = \{g \in G \,|\, ig = i\}$.

G_i is a subgroup of G (why?)

$G_1 = \{1, (345), (354)\}$ Notice: $|G_1| \cdot |1^G| = 3 \times 2 = 6 = |G|$

Orbits and Stabilisers

$X = \{1, 2, 3, 4, 5\}$ and
$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Orbit of $G \leq \mathrm{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$1^G = 2^G = \{1, 2\}$ and $3^G = 4^G = 5^G = \{3, 4, 5\}$.

Stabiliser in G of i is $G_i = \{g \in G \,|\, ig = i\}$.

G_i is a subgroup of G (why?)

$G_1 = \{1, (345), (354)\}$ Notice: $|G_1| \cdot |1^G| = 3 \times 2 = 6 = |G|$

$G_3 = \{1, (12)\}$ Again: $|G_3| \cdot |3^G| = 2 \times 3 = 6 = |G|$

Orbit-Stabiliser Theorem

For any $G \leq \mathrm{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Orbit-Stabiliser Theorem

For any $G \leq \mathrm{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Proof Write $i^G = \{i_1, \ldots, i_r\}$ and $H = G_i = \{h_1, \ldots, h_s\}$.

Choose elements $g_1 = 1, g_2, \ldots, g_r$ such that $ig_j = i_j$ for each j.

Arrange (some of) the group elements like this.

h_1g_1	h_1g_2		h_1g_r
h_2g_1	h_2g_2		h_2g_r
$\vdots$	$\vdots$	$\ldots$	$\vdots$
h_sg_1	h_sg_2		h_sg_r

Orbit-Stabiliser Theorem

For any $G \leq \mathrm{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Proof Write $i^G = \{i_1, \ldots, i_r\}$ and $H = G_i = \{h_1, \ldots, h_s\}$.

Choose elements $g_1 = 1, g_2, \ldots, g_r$ such that $ig_j = i_j$ for each j.

Arrange (some of) the group elements like this.

h_1g_1	h_1g_2		h_1g_r
h_2g_1	h_2g_2		h_2g_r
$\vdots$	$\vdots$	$\ldots$	$\vdots$
h_sg_1	h_sg_2		h_sg_r

The elements in column j form the coset Hg_j. Every element in Hg_j maps i to i_j. So this table contains exactly $r \cdot s$ distinct elements of G.

Orbit-Stabiliser Proof continued

Claim: every $g \in G$ appears exactly once in this table.

h_1g_1	h_1g_2		h_1g_r
h_2g_1	h_2g_2		h_2g_r
$\vdots$	$\vdots$	$\ldots$	$\vdots$
h_sg_1	h_sg_2		h_sg_r

Find ig. By definition of orbit, $ig \in i^G$ so $ig = i_j$ for some j.

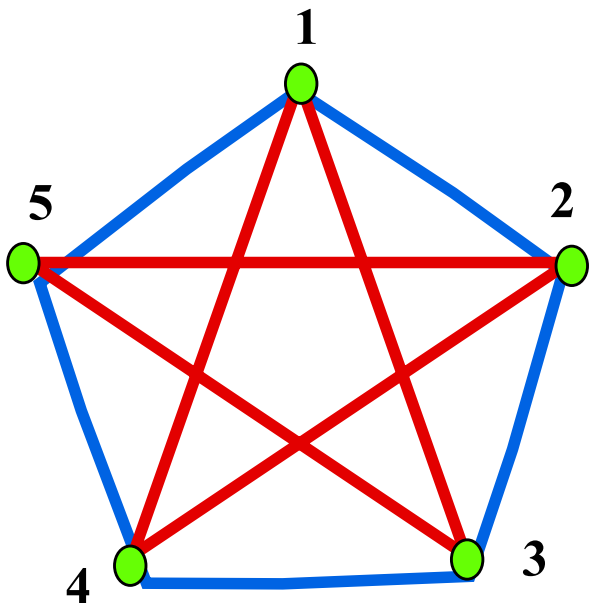
Compute $h := gg_j^{-1}$. (Remember: g first, and then g_j^{-1}.)

Then $h : i \to i$ so $h \in H = G_1$.

Hence $g = hg_j$ lies in column j.
Counting:
$|G|$ = number of elements in the table $= r \cdot s = |i^G| \cdot |G_i|$.

Using the Orbit-Stabiliser Theorem

Let's run through another example: $X = \{1, 2, 3, 4, 5\}$.



$G = \langle (12345), (2354) \rangle$.

$1^G = \{1, 2, 3, 4, 5\}$

Just one G-orbit in X:
G called transitive.

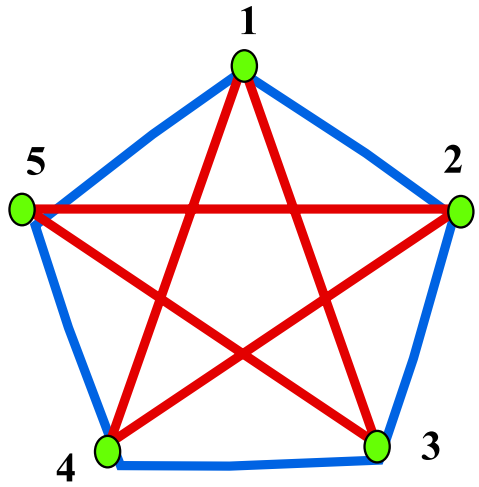
Clearly $(2354) \in G_1$ so
$\langle (2354) \rangle \leq G_1$. Hence $|G_1| \geq 4$.

Use GAP to prove $|G| = 20$.
So $|G_1| = |G|/|1^G| = 20/5 = 4$.
Hence $G_1 = \langle (2354) \rangle$.

Orbit-Stabiliser Theorem for actions

So what's an action? Each element of $G = \langle (12345), (2354) \rangle$

either
{ blue edges } $\leftrightarrow$ { red edges }
or fixes setwise
{ blue edges } and { red edges }



Elements of G induce permutations of $Y = \{$blue edges, red edges $\}$.

We say that G acts on Y (unfaithfully).

The Orbit-Stabiliser theorem also works for actions:

$$|G| = |\text{blue edges}^G| \cdot |G_{\text{blue edges}}| = 2 \times 10.$$

Some GAP code for working with permutation groups

```
gap> a := (1,2);
(1,2)
gap> b := (3,4,5);
(3,4,5)
gap> b^-1;
(3,5,4)
gap> a*b;
(1,2)(3,4,5)
gap> g := Group(a,b);
Group([(1,2),(3,4,5)])
gap> Order(g);
6
```

And GAP code for orbits and stabilisers

gap> Orbit(g, 1);
#This lists the points in the g − orbit containing 1
[1, 2]
gap> Orbits(g); #This list the g − orbits.
[[1, 2], [3, 4, 5]]
We can assign names for lists: gap> o := Orbits(g);
[[1, 2], [3, 4, 5]]
and address various entries in the list: gap> o[1];
[1, 2]
gap> Length(o[1]);
2
gap> g1 := Stabilizer(g, 1);
#GAP returns a set of generators for g1.
Group([(3, 4, 5)])
gap> Order(g1);
3

Two ways to verify with GAP the Orbit-Stabiliser Theorem

```
gap> Order(g1) * Length(Orbit(g, 1));
6
gap> Order(g1) * Length(Orbit(g, 1)) = Order(g);
true
```

One more slide to come on the second example.

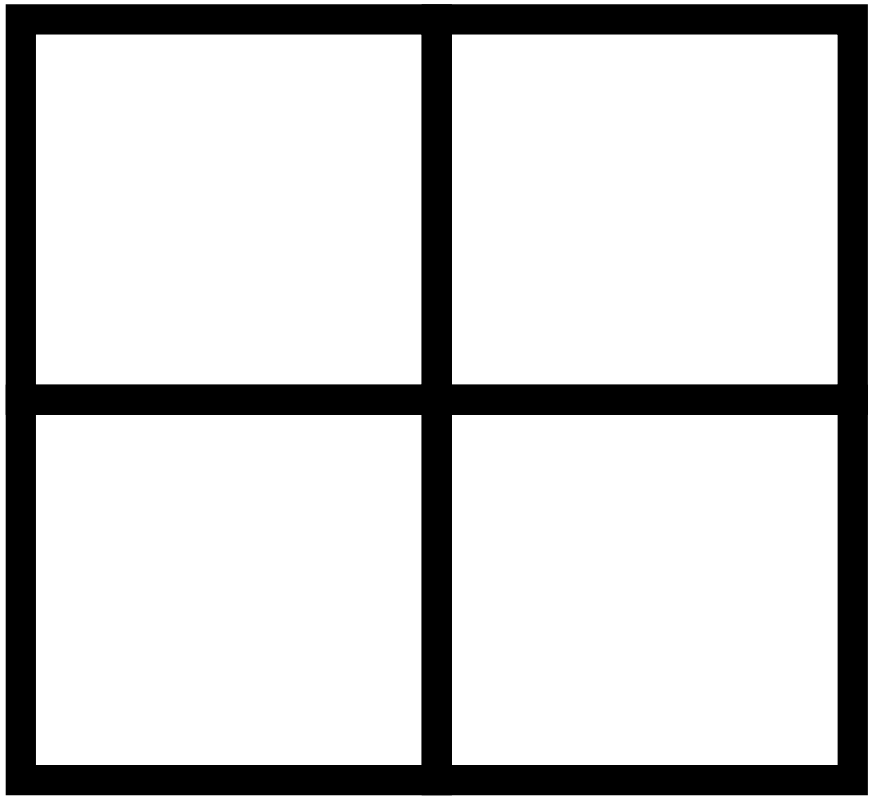
The group on the edge-coloured graph on five vertices

```
gap> a := (1,2,3,4,5);
(1,2,3,4,5)
gap> b := (2,3,5,4);
(2,3,5,4)
gap> G := Group(a,b);
Group([(1,2,3,4,5), (2,3,5,4)])
gap> Order(G);
20
gap> IsTransitive(G);
true
gap> G1 := Stabilizer(G,1);
gap> Order(G1);
4
```

Exercise: Check the Orbit stabiliser Theorem.

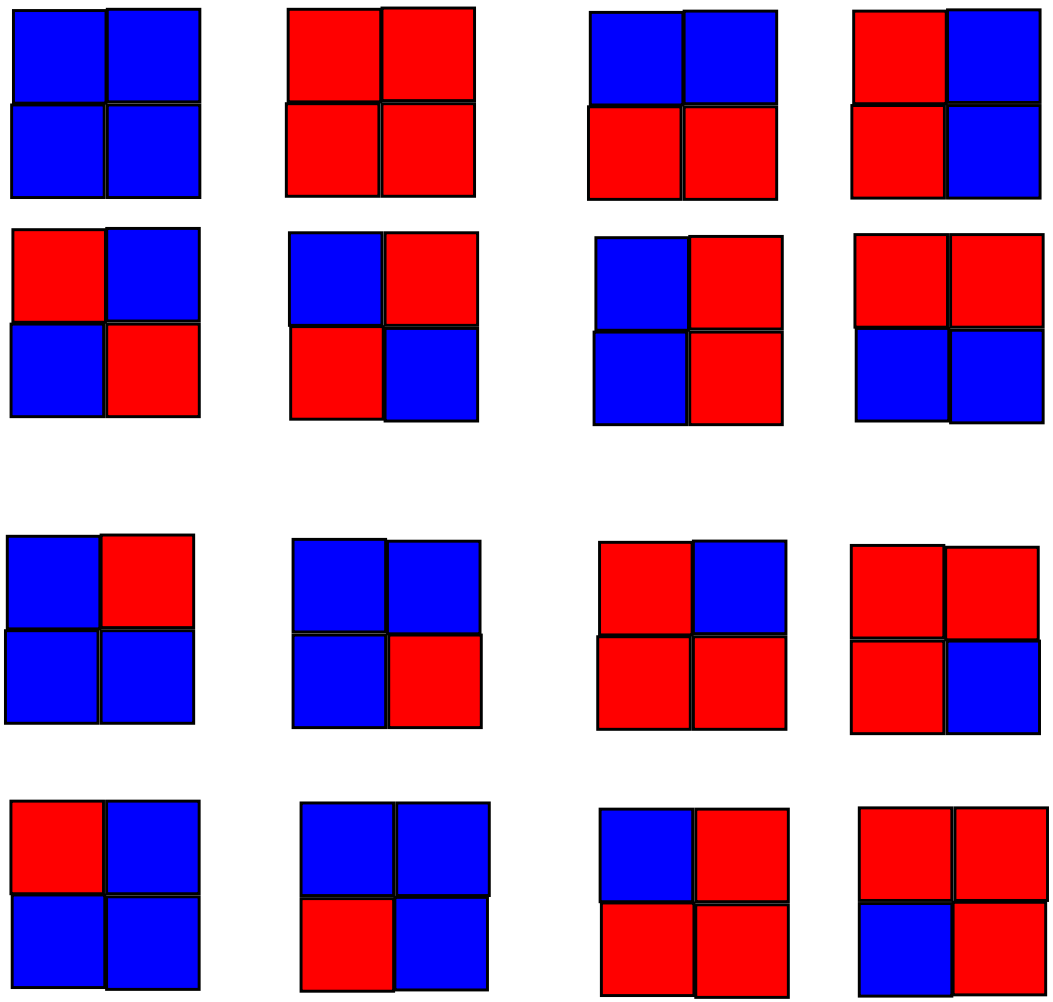
Colouring a grid

In how many different ways can we colour the squares of a 2×2 grid using the colours red and blue?



There are 4 cells and 2 colours; so the number should be $2^4 = 16$.

Here they are



How many coloured grids modulo rotations?

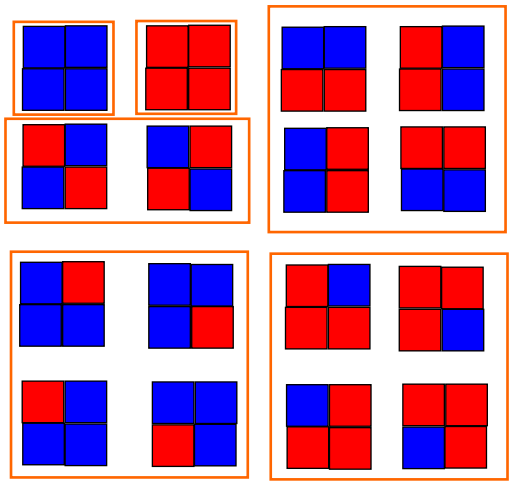
Now suppose that we are allowed to rotate the coloured grids about their centre through $\pi/2, \pi, 3\pi/2, 2\pi$. Some grids will become "indistinguishable from" other grids.

We have just changed the meaning of "different". Now how many different coloured grids are there?

How many coloured grids modulo rotations?

Now suppose that we are allowed to rotate the coloured grids about their centre through $\pi/2, \pi, 3\pi/2, 2\pi$. Some grids will become "indistinguishable from" other grids.

We have just changed the meaning of "different". Now how many different coloured grids are there?



Exactly 6. What's going on? How can we compute this number without drawing all 16 coloured grids?

Characters in our drama

Group G consisting of four rotations.

Set S consisting of 16 coloured grids.

G acts on the set S, and

Coloured grids A and B are "indistinguishable" $\Leftrightarrow$ we can map A to B under some rotation in G.

In other words, A and B are "indistinguishable" $\Leftrightarrow$ A and B lie in the same G-orbit in S.

Thus the number of different/indistinguishable coloured grids modulo the rotation group G is equal to the number of G-orbits in S. We would like an easy way to find the number of G-orbits.

Some challenge questions to keep in mind

Suppose you had 3 different colours.

How many coloured grids? $3^4 = 81$

How many different ones up to rotation? i.e. what is the number of orbits under the rotation group?

How many different coloured grids up to rotation if we use k colours?

How many coloured grids up to rotation and/or reflection if we use k colours?

What if we consider $n \times n$ grids in each of these questions?

Orbit Counting Lemma

Let $G \leq \mathrm{Sym}(X)$.

For $g \in G$ let $\mathrm{fix}(g) =$ number of $x \in X$ such that $xg = x$.
i.e. $\mathrm{fix}(g)$ is the number of fixed points of g in X.

Then the number of G-orbits in X

$$\begin{aligned} &= \text{average of } \mathrm{fix}(g) \text{ over all } g \in G \\ &= \frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g) \end{aligned}$$

Proof of Orbit Counting Lemma

Special Case: G is transitive.
Powerful combinatorial technique:
count pairs (i, g) in two ways $(i \in X, g \in G, ig = i)$.

First count: each $g \in G$ paired with $\text{fix}(g)$ points $i \in X$ with $ig = i$
So number of pairs is $\sum_{g \in G} \text{fix}(g)$.

Second count: each $i \in X$ paired with $|G_i|$ elements $g \in G_i$.
So number of pairs is $\sum_{i \in X} |G_i|$.

Orbit Stabiliser Theorem gives: $|G_i| = \frac{|G|}{|i^G|} = \frac{|G|}{|X|}$ for each i
(because G is transitive). Hence $\sum_{i \in X} |G_i| = |X| \cdot \frac{|G|}{|X|} = |G|$.

Equate results of first and second counts and get:
$\frac{1}{|G|} \sum_{g \in G} \text{fix}(g) = 1$ (the number of orbits for G transitive).

Proof of Orbit Counting Lemma Continued

General Case: G has $t \geq 2$ orbits $X_1, X_2, \ldots, X_t$.
Let $\text{fix}_i(g) =$ the number of fixed points of g in X_i.
So $\text{fix}(g) = \sum_{1 \leq i \leq t} \text{fix}_i(g)$.

Then G acts on X_i with one orbit (transitive) and since the Orbit Stabiliser Theorem applies to actions, the result for the "Special Case" gives:

$$\frac{1}{|G|} \sum_{g \in G} \text{fix}_i(g) = 1$$

for each i so

$$\frac{1}{|G|} \sum_{g \in G} \text{fix}(g) = \frac{1}{|G|} \sum_{g \in G} \text{fix}_1(g) + \cdots + \frac{1}{|G|} \sum_{g \in G} \text{fix}_t(g) = t$$

Revisiting coloured grids

Let $R =$ clockwise rotation through $\pi/2$, and let $G\{R, R^2, R^3, R^4 = 1\}$.

grids fixed by R	$bbbb$ and $rrrr$	2
grids fixed by R	$bbbb$, $rrrr$, $brbr$, $rbrb$	4
grids fixed by R^3	$bbbb$ and $rrrr$	2
grids fixed by $R^4 = 1$	all of them	16
Summing:	$\sum \text{fix}(R^i) =$	24

So $\frac{1}{|G|} \sum_{1 \leq i \leq 4} \text{fix}(R^i) = \frac{1}{4} \cdot 24 = 6$.

Exercises I:

Exercise: Compute the number of different red-blue-green coloured 2×2 grids up to rotation.

Exercise: Find a formula for the number of different red-blue coloured $n \times n$ grids up to rotation (about the centre of the grid).

Exercise: Finish the GAP exercise for the group on the edge-coloured graph on five vertices.

Exercises II

GAP Exercise: Type into GAP: g := `MathieuGroup(11);`
g is a permutation group on $X = \{1, 2, \ldots, 11\}$.

- Decide if g is transitive. Also find the order of g.
- Find g1 the stabiliser of the point 1. Decide if g1 is transitive on $X \setminus \{1\}$.
- Find g12 the stabiliser of the points 1 and 2 (or the stabiliser in g1 of the point 2). Decide if g12 is transitive on $X \setminus \{1, 2\}$.
- Similarly find g123 the stabiliser in g12 of the point 3. Decide if g123 is transitive on $X \setminus \{1, 2, 3\}$.
- Repeat for the points 4 and 5. Make sense of your answers in terms of the Orbit Stabiliser Theorem.
- This "remarkable group" was discovered by Mathieu in the 19^{th} century.