Visual Algebra

Lecture 2.5: Groups of permutations

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Groups of permutations

Loosely speaking, a permutation is an action that rearranges a set of objects.

Definition

Let X be a set. A permutation of X is a bijection $\pi\colon X \to X$.

Definition

The permutations of a set X form a group that we denote S_X or $\mathbf{Perm}(S)$. The special case when $X = \{1, \ldots, n\}$ is called the symmetric group, denoted S_n.

If $|X| = |Y|$, then $S_X \cong S_Y$, so we'll usually work with S_n, which has order $n! = n(n-1)\cdots 2 \cdot 1$.

There are several notations for permutations, each with their strengths and weaknesses.

This is best seen with an example:

i	1	2	3	4	5	6
$\pi(i)$	2	3	1	6	5	4

"*one-line notation*"

"*permutation diagram*"

$$\pi = (1\,2\,3)\,(4\,6)$$

"*cycle notation*"

Permutation notations

One-line notation: $\pi = 231654, \qquad \sigma = 564123$

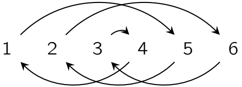
Pros:

- concise
- nice visualization of rearrangement

Cons:

- bad for combining permutations
- not clear where elements get mapped
- hard to compute the inverse

Permutation diagram: π: 

σ: 

Pros:

- can see where elements get mapped
- easy to compute inverses
- convenient for combining permutations

Cons:

- cumbersome to write
- can get tangled

Cycle notation: $\pi = (1\,2\,3)\,(4\,6), \qquad \sigma = (1\,5\,2\,6\,3\,4)$;

Pros:

- short and concise
- easy to see the disjoint cycles
- convenient for combining permutations

Cons:

- representation isn't unique
- not clear what n is

Cycle notation

The cycle $(1\,4\,6\,5)$ means

"*1 goes to 4, which goes to 6, which does to 5, which goes back to 1.*"

Thus, we can write $(1\,4\,6\,5) = (4\,6\,5\,1) = (6\,5\,1\,4) = (5\,1\,4\,6)$.

To find the inverse of a cycle, write it backwards:

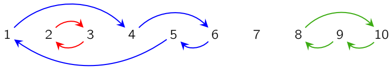
$$(1\,4\,6\,5)^{-1} = (5\,6\,4\,1) = (1\,5\,6\,4) = \cdots$$

Though it's not necessary, we usually prefer to begin a cycle with its smallest number.

Remark

Every permutation in S_n can be written in cycle notation as a product of disjoint cycles, and this is unique up to commuting and cyclically shifting cycles.

For example, consider the following permutation in S_{10}:



as $(1\ 4\ 6\ 5)\,(2\ 3)\,(8\ 10\ 9)$.

This is a product of four disjoint cycles. Since they are disjoint, they commute:

$$(1465)\,(23)\,(8\ 10\ 9) = (23)\,(8\ 10\ 9)\,(1465) = (23)\,(8\ 10\ 9)\,(1465) = \cdots$$

Composing permutations

Remark

The order of a permutation is the least common multiple of the sizes of its disjoint cycles.

For example, $(1\ 3\ 8\ 6)(2\ 9\ 7\ 4\ 10\ 5) \in S_{10}$ has order 12; this should be intuitive.

When cycles are not disjoint, order matters.

Many books compose permutations from right-to-left, due to function composition.

Since we have been using right Cayley graphs, we will compose them from left-to-right.

Notational convention

Composition of permutations will be done left-to-right. That is, given $\pi, \sigma \in S_n$,

$$\pi\sigma \quad \text{means "}\textit{do } \pi\textit{, then do } \sigma\text{".}$$

The main drawback about our convention is that it does not work well with function notation applied to elements, like $\pi(i)$.

For example, notice that

$$(\pi\sigma)(i) = \sigma(\pi(i)) \neq \pi(\sigma(i)).$$

However, we will hardly ever use this notation, so that drawback is minimal.

Composing permutations

Here are two ways illustrating how permutations are composed, with the example

First do

i	1	2	3	4	5	6
$\pi(i)$	4	3	1	2	6	5

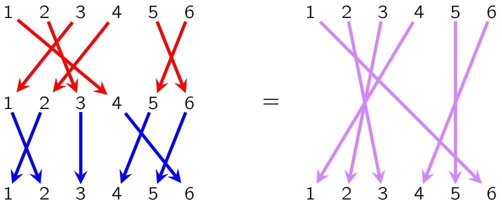
then do

i	1	2	3	4	5	6
$\sigma(i)$	2	1	3	6	4	5

- "By stacking:"

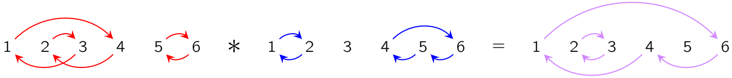
first (1423)(56)

then (12)(465)



(164)(23)

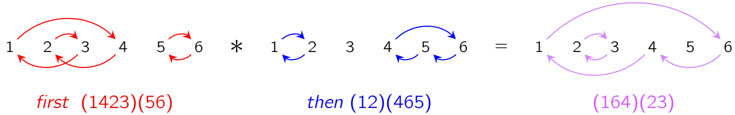
- "By cycles:"



first (1423)(56) *then* (12)(465) (164)(23)

Composing permutations in cycle notation

Let's practice composing two permutations:



Let's now do that in slow motion.

In the example above, we start with 1 and then read off:

- "**1** goes to 4, then 4 goes to 6"; Write: (1 6
- "6 goes to 5, then 5 goes to 4"; Write: (1 6 4
- "4 goes to 2, then 2 goes to **1**"; Write: (1 6 4), and start a new cycle.
- "**2** goes to 3, then 3 is fixed"; Write: (1 6 4) (2 3
- "3 goes to 1, then 1 goes to **2**"; Write: (1 6 4) (2 3), and start a new cycle.
- "**5** goes to 6, then 6 goes to **5**"; Write: (1 6 4) (2 3) (5); now we're done.

We typically omit 1-cycles (fixed points), so the permutation above is just (1 6 4) (2 3).

Permutation matrices

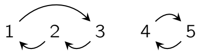
We have seen how to represent groups of symmetries such as V_4, C_n, and D_n as matrices.

Permuting coordinates of $\mathbb{R}^n$ is also a linear transformation.

Every permutation can represented by an $n \times n$ permutation matrix, P_π.

For an example of this, consider the following permutation $\pi \in S_5$:

i	1	2	3	4	5
$\pi(i)$	3	1	2	5	4



$$\pi = (1\,3\,2)\,(4\,5)$$

The matrix P_π permutes the entries of a colum vector:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \\ x_5 \\ x_4 \end{bmatrix},$$

It permutes the entries of a row vector (by coordinates):

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} x_2 & x_3 & x_1 & x_5 & x_4 \end{bmatrix}.$$

Permutation matrices

Definition

Given an element $\pi \in S_n$, the corresponding permutation matrix is the $n \times n$ matrix

$$P_\pi = (p_{ij}), \qquad p_{ij} = \begin{cases} 1 & \pi(i) = j \\ 0 & \text{otherwise.} \end{cases}$$

Here are several more examples of permutation matrices.

$$P_{(12)(34)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_{(134)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad P_{(1234)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Notice that the difference between left and right multiplication is:

$P_\pi P_\sigma x$ Right-to-left: "*Start with x, apply σ, then π*"

$x^T P_\pi P_\sigma$ Left-to-right: "*Start with x^T, apply π, then σ*"

It does not matter whether we use row or column vectors, but we must be careful.

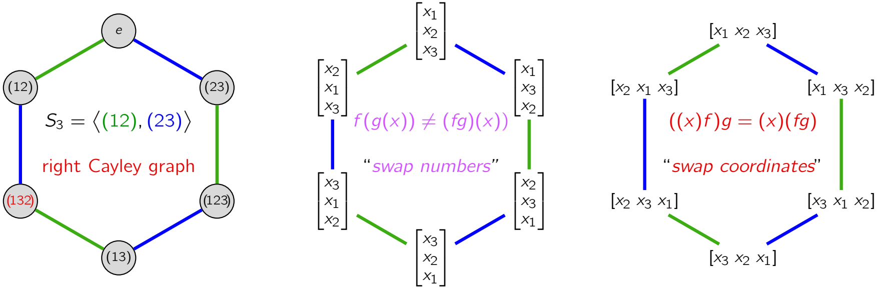
- Column vectors correspond to multiplying right-to-left, as in function composition.
- Row vectors correspond to multiplying left-to-right, which has been our standard.

Our left-to-right multiplication convention is more compatible with row vectors

$$P_{(12)}P_{(23)}\mathbf{v} = \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix} = \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix} = \begin{bmatrix}x_3\\x_1\\x_2\end{bmatrix} = P_{(132)}\mathbf{v}.$$

$$\mathbf{v}^T P_{(12)}P_{(23)} = \begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix} = \begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

$$= \begin{bmatrix}x_2 & x_3 & x_1\end{bmatrix} = \mathbf{v}^T P_{(132)}.$$



Cayley's theorem

A set of permutations that forms a group is called a permutation group.

A fundamental theorem by British mathematician Arthur Cayley (1821–1895) says that every finite group can be thought of as a collection of permutations.

This is clear for groups of symmetries like V_4, C_n, or D_n, but less so for groups like Q_8.

Cayley's theorem

Every finite group is isomorphic to a collection of permutations, i.e., some subgroup of S_n.

We don't have the mathematical tools to prove this, but we'll get a 1-line proof when we study group actions.

A natural first question to ask is the following:

Given a group, how do we associate it with a set of permutations?

We'll see two algorithms which give strong intuition for why Cayley's theorem is true.

Constructing permutations from a Cayley graph

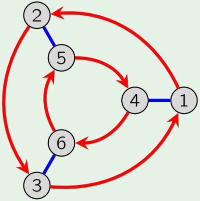
Here is an algorithm given a Cayley graph with n nodes:

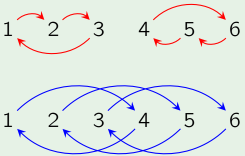
1. number the nodes 1 through n,
2. interpret each arrow type in the Cayley graph as a permutation.

Take the permutations corresponding to the generators.

Example

Let's try this with $D_3 = \langle r, f \rangle$.





We see that D_3 is isomorphic to the subgroup $\big\langle (123)(465),\ (14)(25)(36) \big\rangle$ of S_6.

Constructing permutations from a Cayley table

Here is an algorithm given a Cayley table with n elements:

1. replace the table headings with 1 through n,
2. make the appropriate replacements throughout the rest of the table,
3. interpret each row (or column) as a permutation.

Take the permutations corresponding to *any* generating set.

Example

Let's try this with the Cayley table for $D_3 = \langle r, f \rangle$.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

Row 1 (1):

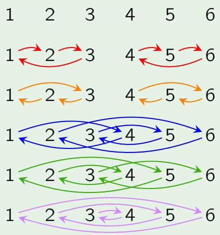
Row 2 (r):

Row 3 (r^2):

Row 4 (f):

Row 5 (rf):

Row 6 $(r^2 f)$:



We see that D_3 is isomorphic to the subgroup $\langle (123)(456), (14)(26)(35) \rangle$ of S_6.