Group Theory Through Permutation Puzzles

[Applied Algebra]

Giovanni Viglietta

University of Aizu – November 29, 2022

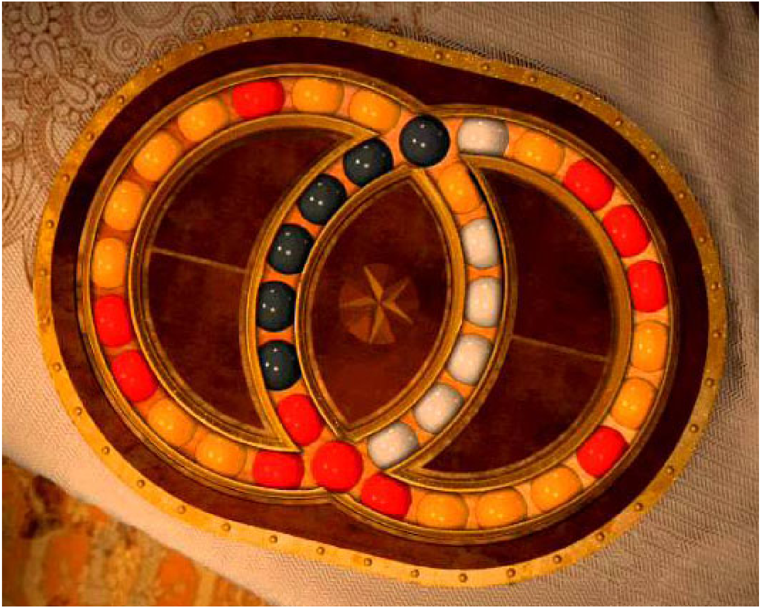
Cyclic-shift puzzles

Cyclic-shift puzzles

Cyclic-shift puzzles

Cyclic-shift puzzles

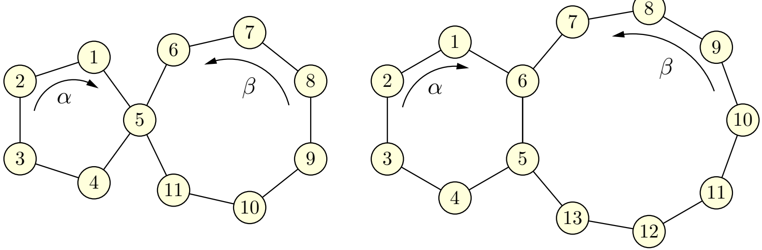
Cyclic-shift puzzles



Cyclic-shift puzzles

Case study: 1-connected and 2-connected puzzles

We focus on cyclic-shift puzzles of two types:



1-connected 2-connected

Our questions are:

- What configurations are reachable from a given initial configuration? (I.e., what is the *configuration space*?)
- How can we get from an initial configuration to a goal configuration in a small number of moves?

Note: we assume that all tokens have <u>distinct colors</u> (or labels).

Overview

Theory

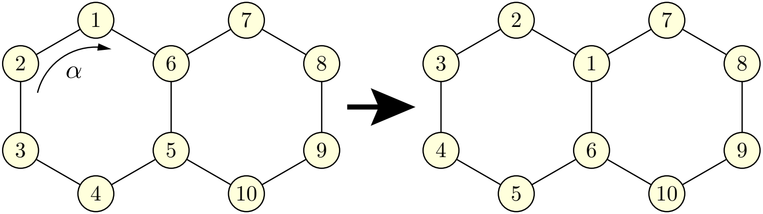
- Groups of permutations
- Subgroups and Lagrange's theorem
- Symmetric and alternating groups
- Conjugation
- Inner and outer automorphisms

Applications

- Solving 1-connected puzzles
- Solving 2-connected puzzles
- Special case: 2-connected puzzle with two 4-cycles

Permutations

Any sequence of moves yields a *permutation* of the tokens:



To represent this permutation, we can use *Cauchy's notation*:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 5 & 6 & 1 & 7 & 8 & 9 & 10 \end{pmatrix}$$

Alternatively, we can use the more compact notation:

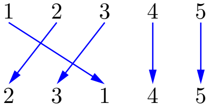
$$[\ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 1\ \ 7\ \ 8\ \ 9\ \ 10\ ]$$

meaning that the first "slot" contains token $\#2$, etc.

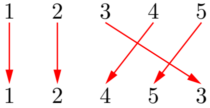
Composition of permutations

Since a permutation is a *bijection* $\pi\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$, permutations can be composed like functions:

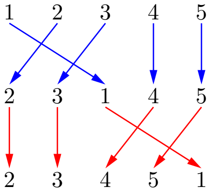
π =



σ =



$\pi\sigma$ =



We can also write it as: $[\,2\ 3\ 1\ 4\ 5\,]\ [\,1\ 2\ 4\ 5\ 3\,] = [\,2\ 3\ 4\ 5\ 1\,]$.

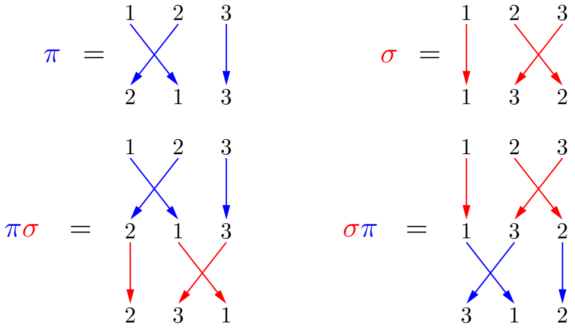
Composition of permutations

Since the composition of functions is associative, we have:

Observation

The composition of permutations is **associative***:* $\pi(\sigma\rho) = (\pi\sigma)\rho$.

The composition of permutations is *not commutative* in general:



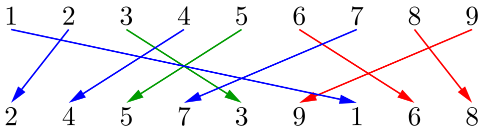
That is, $[2\ 1\ 3]\ [1\ 3\ 2] = [2\ 3\ 1] \neq [3\ 1\ 2] = [1\ 3\ 2]\ [2\ 1\ 3]$.

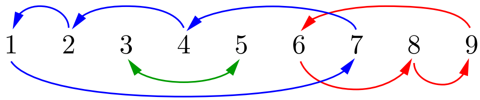
Cycle decomposition

Observation

Every permutation can be expressed as the composition of disjoint cycles in a unique way (up to reordering).

Example:





In compact notation, $[\,2\ 4\ 5\ 7\ 3\ 9\ 1\ 6\ 8\,] = (1\ 2\ 4\ 7)(3\ 5)(9\ 8\ 6)$.

Groups of permutations

The notion of *group* was first formulated by Galois in the 1830s.

Definition

A non-empty set G of permutations of n objects forms a **permutation group** if it is closed under composition:

$$\pi, \sigma \in G \implies \pi\sigma \in G$$

The number of permutations in G is called the *order* of G.
(Not to be confused with n, which is the *degree* of G.)

Observation

The set of all permutations of $\{1, \ldots, n\}$ *forms a group called the* **symmetric group** S_n. *Its order is* $|S_n| = n!$

Identity and inverses

Proposition

Every group G of degree n contains:

- *the* **identity** *permutation $e = [1\ 2\ \ldots\ n]$ and*
- *the* **inverse** *of every element: $\pi \in G \implies \pi^{-1} \in G$,*

where π^{-1} is defined as the permutation such that $\pi\pi^{-1} = e$.

Proof. If $\pi \in G$, then repeatedly composing π with itself eventually reaches $\pi^k = e \in G$, and thus $\pi^{k-1} = \pi^{-1} \in G$. $\square$

Example: If $\pi = (1\ 2\ 3)(4\ 5)$, then $k = \mathrm{lcm}(3,2) = 6$.

$$\begin{aligned}
\pi &= [2\ 3\ 1\ 5\ 4] \\
\pi^2 &= [3\ 1\ 2\ 4\ 5] \\
\pi^3 &= [1\ 2\ 3\ 5\ 4] \\
\pi^4 &= [2\ 3\ 1\ 4\ 5] \\
\pi^5 &= [3\ 1\ 2\ 5\ 4] = \pi^{-1} \\
\pi^6 &= [1\ 2\ 3\ 4\ 5] = e
\end{aligned}$$

Subgroups

Definition

If H and G are groups and $H \subseteq G$, then H is a **subgroup** of G.

If H is a subgroup of G, we write $H \leq G$.

Theorem (Lagrange, 1771)

If $H \leq G$, then the order $|G|$ is a multiple of $|H|$.

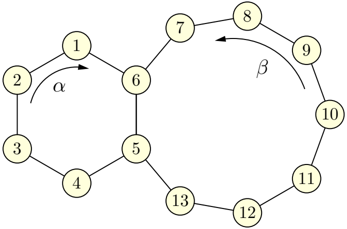
Proof. G is the disjoint union of "copies" of H, called *cosets*. $\square$

$\bullet\ e$ $\quad H$	$\bullet\ \pi_1$ $\quad H\pi_1$	$\bullet\ \pi_2$ $\quad H\pi_2$	$\bullet\ \pi_3$ $\quad H\pi_3$
coset	coset	coset	coset

The number of cosets is called the **index** of H in G.

Generators

Consider the following 2-connected cyclic-shift puzzle:



We have two permutations α and β, the **generators**:

- $\alpha = (1\ 2\ 3\ 4\ 5\ 6)$
- $\beta = (5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13)$

The set of permutations obtained by composing the generators in all possible ways is $\langle \alpha, \beta \rangle$, the group *generated* by α and β.

$$\langle \alpha, \beta \rangle = \{ e,\ \alpha,\ \beta,\ \alpha\alpha,\ \alpha\beta,\ \beta\alpha,\ \beta\beta,\ \ldots,\ \beta\alpha\alpha\beta\beta\alpha\beta\beta\beta,\ \ldots \}$$

$\implies$ Since $\langle \alpha, \beta \rangle$ is a subgroup of S_{13}, its order is a divisor of $13!$

Configuration space

We can now give a description of the **configuration space**.

We know that $\langle \alpha, \beta \rangle$ is a subgroup of S_n: this is the set of permutations that can be obtained starting from the initial permutation $e = [\,1\ 2\ \ldots\ n\,]$.

$\bullet\, e \quad \langle \alpha, \beta \rangle$	$\bullet\, \pi_1 \quad \langle \alpha, \beta \rangle \pi_1$	$\bullet\, \pi_2 \quad \langle \alpha, \beta \rangle \pi_2$	$\bullet\, \pi_3 \quad \langle \alpha, \beta \rangle \pi_3$
coset	coset	coset	coset

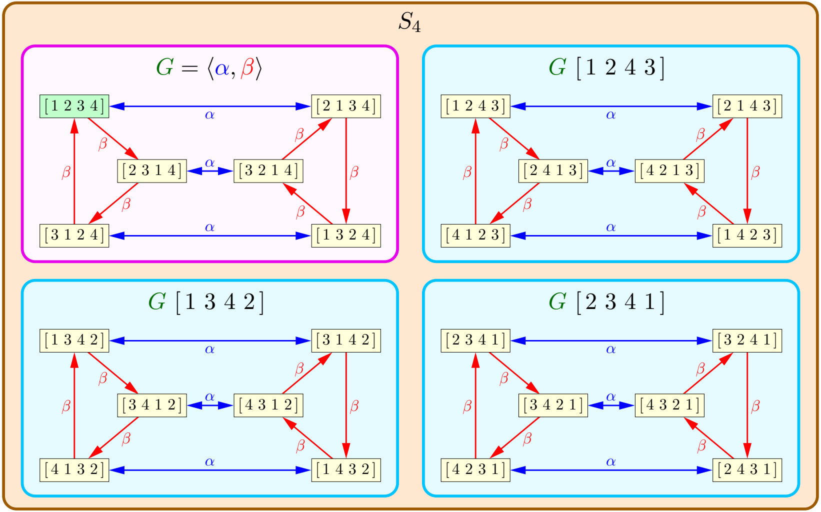
Then there are other copies of $\langle \alpha, \beta \rangle$, all of the same size, corresponding to the other cosets: each is the set of permutations that can be obtained from some initial permutation $\pi_i \notin \langle \alpha, \beta \rangle$.

So, the configuration space can be modeled as a graph with $n! \,/\, |\langle \alpha, \beta \rangle|$ isomorphic connected components: the **Cayley graph**.

$\Longrightarrow$ All we have to do is determine $\langle \alpha, \beta \rangle$.

Cayley graph

Example: The Cayley graph of the subgroup $G \leq S_4$ generated by $\alpha = (1\ 2)$ and $\beta = (1\ 2\ 3)$, as well as its cosets.



Sign of a permutation

Definition

For $\pi \in S_n$, define $\quad \operatorname{sgn}(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(i) - \pi(j)}{i - j}$. $\quad$ (Note: $\operatorname{sgn}(\pi) = \pm 1$.)

Example:

$$\operatorname{sgn}[\,3\ 1\ 4\ 2\,] = \frac{(3-1)(3-4)(3-2)(1-4)(1-2)(4-2)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} = -1$$

Lemma

Transposing any two elements of a permutation changes its sign.

Proof. Transposing a and b in π changes the sign of $(a-b)$. Also, for each c between a and b in π, it changes the sign of $(a-c)$, $(c-b)$. $\square$

Example: $(1\ 2)[\,3\ 1\ 4\ 2\,] = [\,3\ 2\ 4\ 1\,]$;

$$\operatorname{sgn}[\,3\ 2\ 4\ 1\,] = \frac{(3-2)(3-4)(3-1)(2-4)(2-1)(4-1)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} = 1$$

Even and odd permutations

Thus, $\operatorname{sgn}(\pi)$ corresponds to the **parity** (even or odd) of the length of any sequence of transpositions whose composition is π.

Corollary

For any $\pi, \sigma \in S_n$, *we have* $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma)$.

A permutation π is **even** if $\operatorname{sgn}(\pi) = 1$ and **odd** if $\operatorname{sgn}(\pi) = -1$.

Definition

The set of all *even* permutations of $\{1, \ldots, n\}$ forms a group called the **alternating group** $A_n \leq S_n$.

Note: The set O_n of *odd* permutations is not a group (in fact, $e \notin O_n$).

Proposition

A_n *and* O_n *are the two cosets of* A_n *in* S_n. *Thus,* $|A_n| = n!/2$.

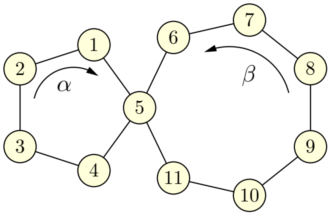
Proof. The function $\pi \mapsto (1\ 2)\pi$ is a bijection between A_n and O_n. $\square$

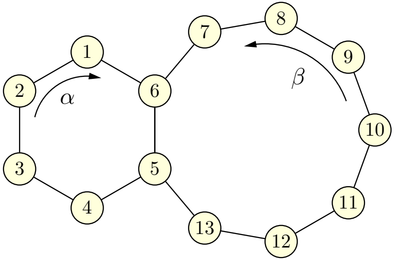
Parity of cycles

Observation

A cycle of length k is the composition of $k-1$ transpositions.

Example: $(1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)$.





So, the two cycles α and β generate a subgroup of A_n if and only if they <u>both</u> have odd length.

Can we prove that α and β generate *exactly* A_n or S_n?

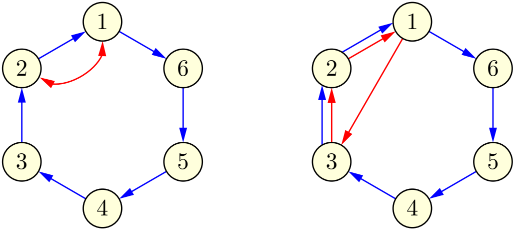
Generators of S_n and A_n

The following facts are folklore, and can be proved by mimicking the *Bubble Sort* algorithm:

Lemma

- $\langle (1\ 2\ \ldots\ n), (1\ 2) \rangle = S_n$.
- $\langle (1\ 2\ \ldots\ n), (1\ 2\ 3) \rangle \geq A_n$.

Any permutation in the group can be generated in $O(n^2)$ steps.



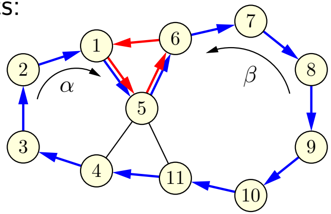
Therefore, if our α and β generate the cycles above, we can conclude that they generate all of S_n or A_n.

Solving 1-connected puzzles

Theorem

In a 1-connected puzzle, α and β generate A_n if they both have odd length, and S_n otherwise.
Any permutation in the group can be generated in $O(n^2)$ steps.

Proof. $\beta^{-1}\alpha$ is an n-cycle and $\alpha\beta\alpha^{-1}\beta^{-1}$ is a 3-cycle of consecutive elements:

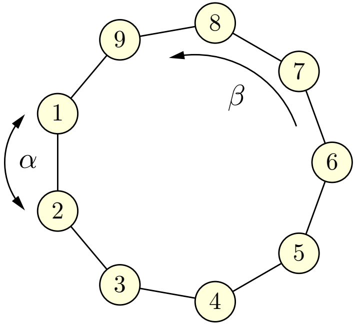


So, $\langle\alpha, \beta\rangle \geq A_n$. If both α and β are even permutations, they cannot generate an odd permutation, and thus $\langle\alpha, \beta\rangle = A_n$.

Say α is odd. We can obtain any odd permutation π by generating the even permutation $\pi\alpha$ (as before), and then doing α^{-1}. $\square$

Trivial 2-connected puzzles

What about 2-connected puzzles? If $\alpha = (1\ 2)$, we already know that the generated group is $\langle\,(1\ 2),\ (1\ 2\ \ldots\ n)\,\rangle = S_n$.



To solve more complex 2-connected puzzles, we use *conjugations*...

Conjugation

Definition

The permutation π, **conjugated** by σ, is the permutation $\sigma\pi\sigma^{-1}$.

The same operation is done in linear algebra when changing coordinates: a linear transformation defined by a matrix A can also be expressed as PAP^{-1}, where P is a nonsingular matrix defining a *change of basis*.

Lemma

Conjugation preserves the **cycle structure** *of permutations.*

Proof. Conjugation permutes labels in the cycle decomposition. $\square$

Example: $(3\ 5\ 7)\,(1\ 3\ 4)(2\ 6)(5\ 7)\,(7\ 5\ 3) = (1\ 5\ 4)(2\ 6)(7\ 3)$.

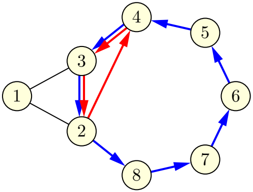
$\implies$ Conjugation allows us to "move cycles around" in a puzzle...

Solving 2-connected puzzles

Theorem

In a 2-connected puzzle with $\alpha = (1\ 2\ 3)$, the generated group is A_n if β has odd length, and S_n if β has even length.
Any permutation in the group can be generated in $O(n^2)$ steps.

Proof. Conjugating α^{-1} by $\alpha^{-1}\beta$, we obtain the 3-cycle $\alpha^{-1}\beta\,\alpha^{-1}\,\beta^{-1}\alpha = (2\ 3\ 4)$ of consecutive elements of β:



So, we can generate any even permutation of $\{2, 3, \ldots, n\}$.

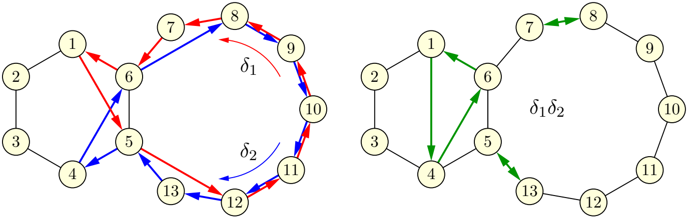
To obtain a given permutation π, first move the correct token $\pi(1)$ in position 1 (possibly shuffling the rest), and then operate on $\{2, 3, \ldots, n\}$ as before (paying attention to parity... details omitted). $\square$

Solving 2-connected puzzles

Theorem

In a 2-connected puzzle, α and β generate A_n if they both have odd length, and S_n otherwise (unless they both have length 4, see later). Any permutation in the group can be generated in $O(n^2)$ steps.

Proof. Conjugating β by $\beta^{-1}\alpha$ and β^{-1} by $\beta\alpha^{-1}$, we obtain two cycles δ_1 and δ_2 of the same length, going in opposite directions:



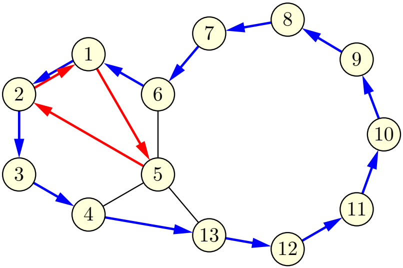
Their composition $\delta_1\delta_2$ is a 3-cycle plus two transpositions.

So, $(\delta_1\delta_2)^2$ is the 3-cycle $(1\ a-2\ a)$, where a is the length of α.

Solving 2-connected puzzles

Proof (continued).

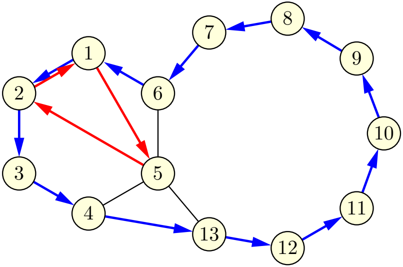
Conjugating $(1\ a-2\ a)$ by α, we obtain the 3-cycle $(1\ 2\ a-1)$.



Note that $(1\ 2\ a-1)$ and $\alpha^{-1}\beta$ form a 2-connected puzzle with a 3-cycle, hence we can apply the previous theorem. $\square$

Proof (continued).

Conjugating $(1\ a-2\ a)$ by α, we obtain the 3-cycle $(1\ 2\ a-1)$.



Note that $(1\ 2\ a-1)$ and $\alpha^{-1}\beta$ form a 2-connected puzzle with a 3-cycle, hence we can apply the previous theorem. □

What about the 2-connected puzzle where α and β have length 4? It looks like we cannot form any 2-cycle or 3-cycle, so we need a radically new idea...

Automorphisms

Definition

An **isomorphism** between two groups G and G' is a bijection $f\colon G \to G'$ such that, for all $\pi, \sigma \in G$, $f(\pi\sigma) = f(\pi)\, f(\sigma)$.

If there is such a bijection f, then G and G' have the same structure: they are "the same group" up to renaming their elements: $G \cong G'$.

Definition

An isomorphism from G to itself is called an **automorphism**.

An automorphism f permutes the elements of G, so $f \in S_{|G|}$.

Proposition

The automorphisms of G form a subgroup $\mathrm{Aut}(G) \leq S_{|G|}$.

Proof. If $f, g \in \mathrm{Aut}(G)$, then $fg(\pi\sigma) = f(g(\pi)g(\sigma)) = fg(\pi)fg(\sigma)$. $\square$

Inner automorphisms

Proposition

The conjugation by an element $\pi \in G$ is an automorphism of G.

Proof. If $f_\pi(\sigma) = \pi\sigma\pi^{-1}$ for all $\sigma \in G$, then $f_\pi \in \mathrm{Aut}(G)$:

$f_\pi(\sigma\rho) = \pi(\sigma\rho)\pi^{-1} = (\pi\sigma\pi^{-1})(\pi\rho\pi^{-1}) = f_\pi(\sigma)\, f_\pi(\rho)$. □

Definition

The automorphisms induced by conjugations are called **inner**.

Proposition

The inner automorphisms form a subgroup $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Proof. If $f_\pi, f_\sigma \in \mathrm{Inn}(G)$, then $f_\pi f_\sigma(\rho) = \pi(\sigma\rho\sigma^{-1})\pi^{-1} = f_{\pi\sigma}(\rho)$. □

Outer automorphisms of S_6

If $n \neq 6$, the only automorphisms of S_n are the inner ones.

S_6 is an exception:

Theorem (Hölder, 1895)

The index of $\mathrm{Inn}(S_6)$ *in* $\mathrm{Aut}(S_6)$ *is 2. So, there are* $6! = 720$ *inner and* 720 *non-inner (i.e., outer) automorphisms.*

This is an example of an **outer automorphism** $\psi \colon S_6 \to S_6$ (defined on a generating set for S_6):

$$\psi((1\ 2)) = (1\ 2)(3\ 5)(4\ 6)$$

$$\psi((2\ 3)) = (1\ 6)(2\ 5)(3\ 4)$$

$$\psi((3\ 4)) = (1\ 2)(3\ 6)(4\ 5)$$

$$\psi((4\ 5)) = (1\ 6)(2\ 4)(3\ 5)$$

$$\psi((5\ 6)) = (1\ 2)(3\ 4)(5\ 6)$$

Solving the last 2-connected puzzle

Theorem

In the 2-connected puzzle where α and β have length 4 (so, $n = 6$), the generated group is isomorphic to S_5 (hence it has index 6).

Proof. Idea: transform $\langle \alpha, \beta \rangle$ by ψ and see what group we obtain.

Since ψ is an *isomorphism*, $\langle \alpha, \beta \rangle \cong \langle \psi(\alpha), \psi(\beta) \rangle$.

$\alpha = (1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4)$ and

$\beta = (3\ 4\ 5\ 6) = (3\ 4)(4\ 5)(5\ 6)$, thus we have:

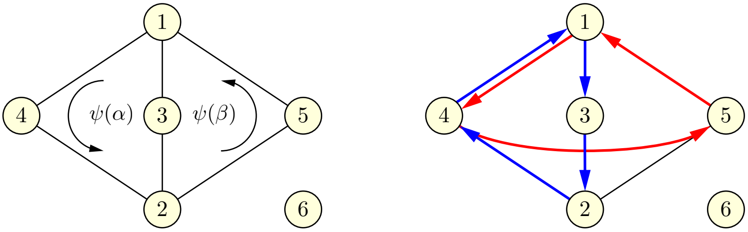
$\psi(\alpha) = \psi((1\ 2))\,\psi((2\ 3))\,\psi((3\ 4)) = (1\ 3\ 2\ 4)$,

$\psi(\beta) = \psi((3\ 4))\,\psi((4\ 5))\,\psi((5\ 6)) = (1\ 5\ 2\ 3)$.

Note: the new generators $\psi(\alpha)$ and $\psi(\beta)$ both <u>leave the token 6 in place</u>, and so they cannot generate a subgroup larger than S_5.

Proof (continued).

The 3-cycle $\psi(\alpha)\,\psi(\beta) = (1\ 5\ 4)$ and the 4-cycle $\psi(\alpha)^{-1}$ form a 2-connected puzzle on $\{1, 2, 3, 4, 5\}$:



By the previous theorem, we know that they generate exactly S_5.

Thus, $\langle \alpha, \beta \rangle$ is an *isomorphic copy* of S_5. A permutation $\pi \in S_6$ is in $\langle \alpha, \beta \rangle$ if and only if $\psi(\pi)$ leaves the token 6 in place. $\square$

Conclusion

We have obtained a complete solution to all 1-connected and 2-connected cycle-shift puzzles:

Theorem

In a 1-connected or 2-connected puzzle, α and β generate:

- A_n *if both* α *and* β *have odd length;*
- S_n *if* α *or* β *has even length, with one exception:*
- *if the puzzle is 2-connected and* α *and* β *have length 4, they generate a group isomorphic to* S_5 *(as opposed to* S_6*).*

Any permutation in the group can be generated in $O(n^2)$ *steps.*