Group Theory Applied to Cyclic-Shift Puzzles

Giovanni Viglietta

(Partially from a joint work with Kwon Kham Sai and Ryuhei Uehara)

JAIST – November 6, 2020

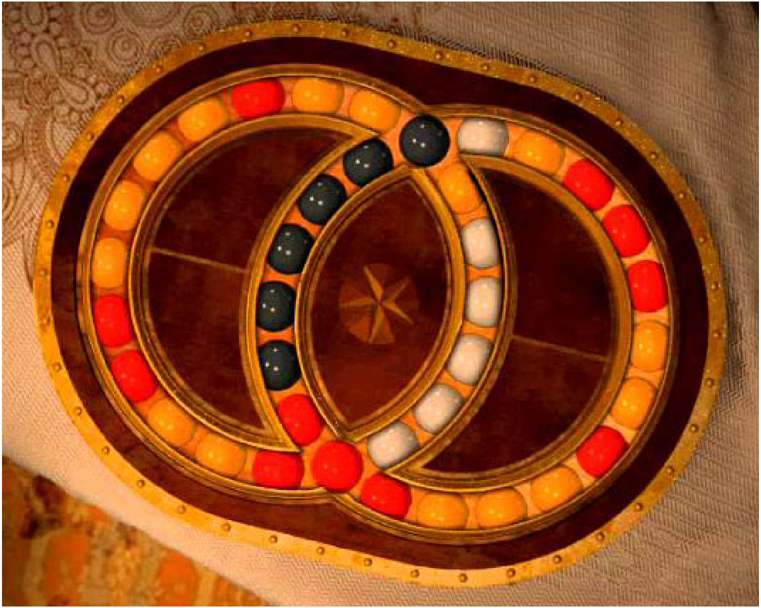
Cyclic-shift puzzles

Cyclic-shift puzzles

Cyclic-shift puzzles

Cyclic-shift puzzles

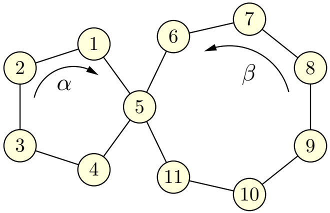
Cyclic-shift puzzles



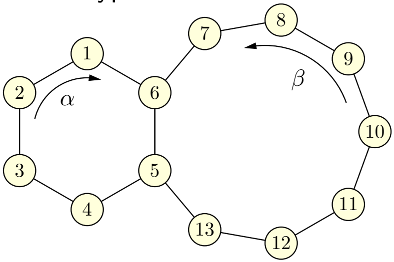
Cyclic-shift puzzles

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 final configuration in an efficient way?

Note: we assume that all tokens have distinct colors.

Overview

Theory

- Groups of permutations
- Lagrange's theorem for subgroups
- Even and odd permutations
- Conjugation
- Automorphisms

Applications

- 1-connected cyclic-shift puzzles
- 2-connected cyclic-shift puzzles
  - Special case with two 4-cycles
- Generalized cyclic-shift puzzles

Permutations

- We can represent any configuration as a *permutation* describing where each token is located.
- Notation: $[3\ 6\ 4\ 1\ 7\ 2\ 5]$ means that the first slot contains token $\#3$, the second slot contains token $\#6$, etc.
- Since a permutation is a *bijection* $\pi\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$, permutations can be composed like functions:
  e.g., $[2\ 3\ 1\ 4\ 5]\,[1\ 2\ 4\ 5\ 3] = [2\ 3\ 4\ 5\ 1]$.
- Composition of permutations is *associative*: $\pi(\sigma\rho) = (\pi\sigma)\rho$.
- Composition of permutations is *not commutative* in general:
  e.g., $[2\ 1\ 3]\,[1\ 3\ 2] = [2\ 3\ 1] \neq [3\ 1\ 2] = [1\ 3\ 2]\,[2\ 1\ 3]$.
- Every permutation can be expressed as the composition of disjoint *cycles* in a unique way:
  e.g., $[3\ 6\ 4\ 1\ 7\ 2\ 5] = (1\ 3\ 4)(2\ 6)(5\ 7)$.

Groups of permutations

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

A non-empty set G of permutations of n objects is a *group* if:

(1) G is closed under composition:
$\pi, \sigma \in G \implies \pi\sigma \in G$,

(2) G is closed under inversion:
$\pi \in G \implies \pi^{-1} \in G$.

Groups of permutations

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

A non-empty set G of permutations of n objects is a *group* if:

(1) G is closed under composition: $\pi, \sigma \in G \implies \pi\sigma \in G$,

(2) G is closed under inversion: $\pi \in G \implies \pi^{-1} \in G$.

- Note: G contains the *identity permutation* $e = [\,1\ 2\ \ldots\ n\,]$, because $\pi \in G \implies \pi^{-1} \in G \implies \pi\pi^{-1} = e \in G$.
- The number of permutations in G is called the *order* of G (not to be confused with n, which is the *degree* of G).
- The set of *all* permutations of $\{1, \ldots, n\}$ forms a group called the *symmetric group* S_n. Its order is $|S_n| = n!$.

Subgroups

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

Theorem (Lagrange)

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

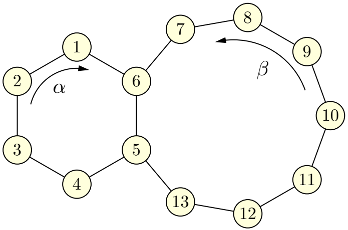
Proof. G is the disjoint union of "copies" of H, called *cosets*. $\square$

$\bullet\, e$ $\quad H$	$\bullet\, \pi_1$ $\quad H\pi_1$	$\bullet\, \pi_2$ $\quad H\pi_2$	$\bullet\, \pi_3$ $\quad H\pi_3$
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 and their inverses, the *generators*:

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

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.

$$\langle \alpha, \beta \rangle = \{ e,\ \alpha,\ \beta,\ \alpha\beta,\ \beta\alpha,\ \alpha^{-1}\beta,\ \ldots,\ \beta^{-1}\alpha\alpha\beta\beta\alpha^{-1}\beta\beta\beta,\ \ldots \}$$

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 $\langle \alpha, \beta \rangle$.

Some known facts

Let a set of of generators P be given as input, and let $G = \langle P \rangle$.
The following problems are solvable in polynomial time (Sims, 1970):

- Compute the order of G.
- Decide if a given permutation π is in G.
- If $\pi \in G$, find an expression for π in terms of the generators.

On the other hand, the minimization problem is hard:

- If $\pi \in G$, finding the shortest sequence of generators whose composition is π is PSPACE-complete (Jerrum, 1985).
- If all the generators in P are cycles, the problem is NP-hard (Sai-Uehara, 2020). It is not known if it is PSPACE-complete.

Moreover, under some conditions that are satisfied by cyclic-shift puzzles,

- The length of a shortest generator sequence for π is upper bounded by a quasi-polynomial function of n (Helfgott-Seress, 2013).
- It is not known if there is a polynomial upper bound. If so, finding the shortest sequence of generators would be in NP.

Even and odd permutations

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

Example: $\mathrm{sgn}[\,3\ 1\ 4\ 2\,] = \frac{(3-1)(3-4)(3-2)(1-4)(1-2)(4-2)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} = -1$.

Even and odd permutations

For $\pi \in S_n$, define $\quad \operatorname{sgn}(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}$. (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 two elements changes the sign of a permutation.

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

For $\pi \in S_n$, define $\quad \operatorname{sgn}(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}$. (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 two elements changes the sign of a permutation.

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

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

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

Another consequence is that $\quad \operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma)$.

So, the *even* permutations (i.e., $\operatorname{sgn}(\pi) = 1$) form a group called the *alternating group* $A_n \leq S_n$. (The *odd* permutations do <u>not</u> form a group.)

Note that $f(\pi) = (1\ 2)\,\pi$ is a *bijection* between even and odd permutations. So, the order of A_n is $n!/2$, and the sets of even and odd permutations are the two *cosets* of A_n in S_n.

Some known facts

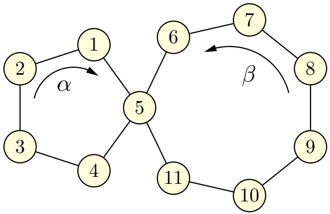
- Two random permutations of n objects generate either S_n or A_n with probability $1 - 1/n + O(n^{-2})$ (Babai, 1989).*
- The permutations π such that $\langle\, (1\ 2\ \ldots\ n),\ \pi\, \rangle$ is S_n or A_n have been characterized (Heath et al., 2009).
- Under some conditions that apply to our cyclic-shift puzzles, if there is a cycle of length $n - 3$ or less, the generated group is S_n or A_n (Jones, 2014).†

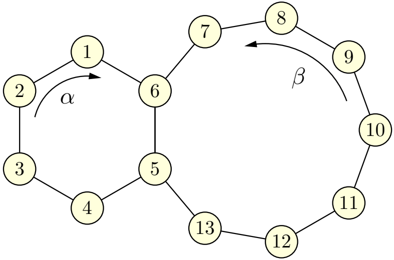
*This says nothing about the special case where the generators are cycles.
†The proof is not self-contained and highly non-constructive.

Parity of cycles

Note: 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:

(1) $\langle\,(1\ 2\ \ldots\ n),\,(1\ 2)\,\rangle = S_n$.

(2) $\langle\,(1\ 2\ \ldots\ n),\,(1\ 2\ 3)\,\rangle \geq A_n$.*

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

$\Longrightarrow$ If our α and β generate the cycles in either (1) or (2), we can conclude that they generate all of S_n or A_n.

---

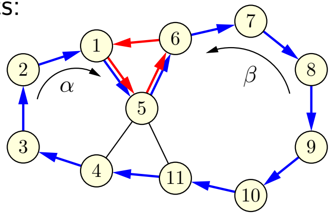
*Obviously, the generated group is S_n if n is even, and A_n if n is odd.

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}. $\square$

Conjugation

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

Conjugation

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

To extend our analysis to other 2-connected puzzles, we use *conjugations*: 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*.

Conjugation

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

To extend our analysis to other 2-connected puzzles, we use *conjugations*: 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*.

Similarly, conjugating a permutation preserves its cycle structure.

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

Conjugating permutes the tokens in the cycle decomposition.

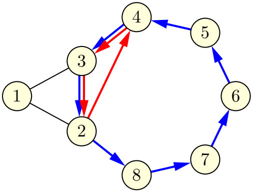
We can use conjugation in our puzzles to "move cycles around"...

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:



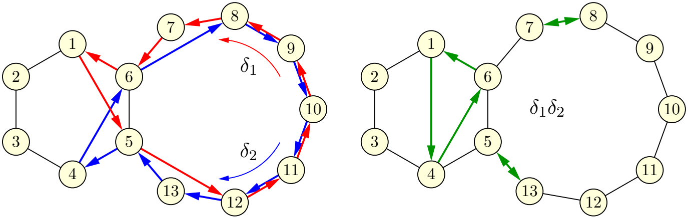
So, we can generate any even permutation of $\{2, 3, \ldots, n\}$.

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). $\square$

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:

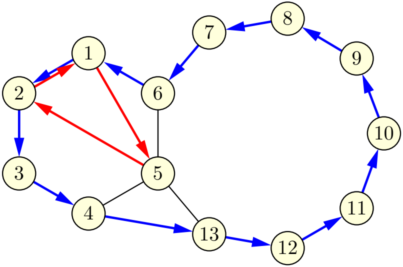


Their composition $\delta_1\delta_2$ is a 3-cycle plus two transpositions.

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

Proof (continued).

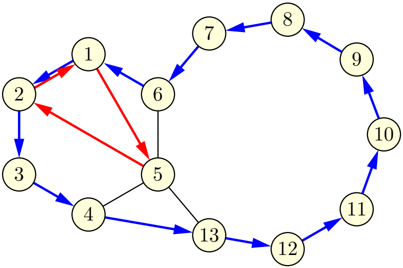
Conjugating $(1\ a-2\ a)$ by α, we obtain the 3-cycle $(1\ 2\ a-1)$.



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

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

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, and we write $G \cong G'$.

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

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

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

Automorphisms

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

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, and we write $G \cong G'$.

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

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

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

Note that conjugation by an element $\pi \in G$ is an automorphism:

if $f_\pi(\sigma) = \pi\sigma\pi^{-1}$ for all $\sigma \in G$, then $f_\pi \in \mathrm{Aut}(G)$, because $f_\pi(\sigma\rho) = \pi(\sigma\rho)\pi^{-1} = (\pi\sigma\pi^{-1})(\pi\rho\pi^{-1}) = f_\pi(\sigma)\, f_\pi(\rho)$.

The automorphisms induced by conjugations are called *inner*, and they form a subgroup $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Outer automorphisms of S_6

If $n \neq 6$, the only automorphisms of S_n are the inner ones.
So, we have $\mathrm{Inn}(S_n) = \mathrm{Aut}(S_n)$ if $n \neq 6$.*

S_6 is an exception: the index of $\mathrm{Inn}(S_6)$ in $\mathrm{Aut}(S_6)$ is 2, so there are $6! = 720$ *inner* and 720 *outer* automorphisms (Hölder, 1895).

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

$$\begin{aligned}
\psi((1\ 2)) &= (1\ 2)(3\ 5)(4\ 6),\\
\psi((2\ 3)) &= (1\ 6)(2\ 5)(3\ 4),\\
\psi((3\ 4)) &= (1\ 2)(3\ 6)(4\ 5),\\
\psi((4\ 5)) &= (1\ 6)(2\ 4)(3\ 5),\\
\psi((5\ 6)) &= (1\ 2)(3\ 4)(5\ 6).
\end{aligned}$$

*Actually, if $n \neq 2$ and $n \neq 6$, then $\mathrm{Aut}(S_n) \cong S_n$.

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:

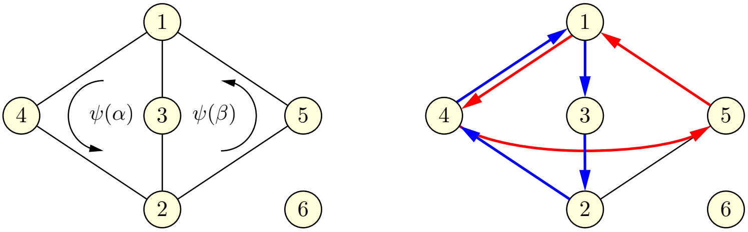
$\psi(\alpha) = \psi((1\ 2))\,\psi((2\ 3))\,\psi((3\ 4)) = (1\ 3\ 2\ 4)$,

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

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.

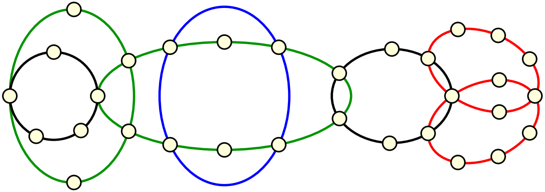
Thus, $\langle \alpha, \beta \rangle$ is an *isomorphic copy* of S_5. A permutation $\pi \in S_6$ is in $\langle \alpha, \beta \rangle$ if and only if $\psi(\pi)$ leaves the token 6 in place. $\square$

Generalized cyclic-shift puzzles

Let $\mathcal{C}$ be a set of cycles, and let $\hat{G} = (\mathcal{C}, \mathcal{E})$ be the graph where $\{C_1, C_2\} \in \mathcal{E}$ if C_1 and C_2 induce a 1- or a 2-connected puzzle.

$\mathcal{C}$ forms a *proper cyclic-shift puzzle* if there is $\mathcal{C}' \subseteq \mathcal{C}$ such that:

- $\mathcal{C}'$ contains at least two cycles.
- The induced subgraph $\hat{G}[\mathcal{C}']$ is connected.
- Each token is contained in at least one cycle in $\mathcal{C}'$.



Theorem

The configuration group of a proper cyclic-shift puzzle with more than 6 tokens is A_n if all cycles have odd length, and S_n otherwise. Any permutation in the group can be generated in $O(n^5)$ steps.

Open problems

(1) Improve the $O(n^5)$ upper bound in the last theorem.

(2) Extend the analysis to cyclic-shift puzzles that are not proper.

(3) What about puzzles where tokens may have the same color?

(4) Is the minimization problem PSPACE-complete for cycles?

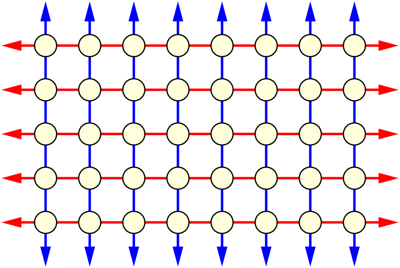
(5) Is it NP-hard for planar graphs?

(6) Is it NP-hard for complete graphs?

(7) Is it NP-hard for graphs of small maximum degree?

Torus puzzle

The *torus puzzle* is a good candidate for settling open problem (7), as its graph is 4-regular, as well as toroidal and vertex-transitive:



Since it is a *proper* cyclic-shift puzzle, we know how to solve it...

But solving the torus puzzle in the minimum number of moves is NP-hard (by a reduction from 3-Partition) even if the tokens have only *two* possible colors (Amano et al., 2012).

However, consecutive shifts along the same cycle count as 1 move!

Does the reduction extend to our model of cyclic-shift puzzles?

References

K. Amano, Y. Kojima, T. Kurabayashi, K. Kurihara, M. Nakamura, A. Omi, T. Tanaka, and K. Yamazaki
How to solve the torus puzzle
Algorithms 5(1):18–29, 2012

L. Babai
The probability of generating the symmetric group
Journal of Combinatorial Theory (Series A), 52:148–153, 1989

D. Heath, I. M. Isaacs, J. Kiltinen, and J. Sklar
Symmetric and alternating groups generated by a full cycle and another element
The American Mathematical Monthly, 116(5):447–451, 2009

H. A. Helfgott and A. Seress
On the diameter of permutation groups
Annals of Mathematics, 179(2):611–658, 2014

References

M. R. Jerrum
The complexity of finding minimum-length generator sequences
Theoretical Computer Science, 36:265–289, 1985

G. A. Jones
Primitive permutation groups containing a cycle
Bulletin of the Australian Mathematical Society,
89(1):159–165, 2014

J. J. Rotman
An introduction to the theory of groups
Springer-Verlag, 4th edition, 1995

K. K. Sai, R. Uehara, and G. Viglietta
Cyclic shift problems on graphs
arXiv:2009.10981, 2020

C. Sims
Computational problems in abstract algebra
Ed. John Leech, Pergamon Press, 1970