Permutation Basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
22 October, 2023 (at *10:05*)

Please learn pages 1–3.

Permutations

On a set Ω, a bijection $\pi{:}\Omega{\to}\Omega$ is also called a "***permutation*** of Ω". Use ***perm*** to abbrev. "permutation". A ***token*** is an element $x \in \Omega$. Use Id_Ω for the identity perm, $x \mapsto x$.

Composition. It will be convenient to have symbols for composition in *both* directions. Use $\triangleleft$ as a synonym of $\circ$. Thus

1a: *Both* $[\alpha \triangleright \beta](x)$ *and* $[\beta \triangleleft \alpha](x)$ *mean* $\beta(\alpha(x))$.

[Think of the triangle as *pointing* in the direction of data-flow.] Use $\beta^{\circ n}$ for "the n^{th}***-composition-power*** of β". E.g

1b: $$\beta^{\circ 3}(x) \;=\; \beta\Big(\beta(\beta(x))\Big)\,,$$

and $\beta^{\circ -1}$ is the ***inverse function*** of β, which we will usually just write as β^{-1}. When composition is understood, we will write β^3 rather than $\beta^{\circ 3}$.

The $\mathbb{S}_\Omega$ group. The set all permutations on Ω is "the ***symmetric group*** on Ω", written $\mathbb{S}_\Omega$.

DEFN: *We will view permutation-composition as going L-to-R; permutation* $\alpha\beta$ *is* $\alpha \triangleright \beta$*, first applying* α*, then* β*. So* $[\alpha\beta](x)$ *is* $\beta(\alpha(x))$.

Hence triple $\big(\mathbb{S}_\Omega, \triangleright, Id_\Omega\big)$ *is a group.*

NOTE: Our L-to-R convention for permutations is the *opposite* of Gallian's textbook, but *agrees* with the convention used in Prof. Miklos Bona's Combinatorics text, which you may be using next semester.

Orbits. For $\beta \in \mathbb{S}_\Omega$, "the β***-orbit*** of token x" is the set

$$\mathcal{O}_\beta(x) \;:=\; \{\beta^{\circ k}(x) \mid k \in \mathbb{Z}\}\,,$$

together with the information that β maps $\beta^{\circ k}(x)$ to $\beta^{\circ[k+1]}(x)$. A β-orbit is either *finite* [a K-cycle for some posint K], or is *infinite*, and is thus a copy of the add-one function mapping $\mathbb{Z}{\to}\mathbb{Z}$. This last is an "$\infty$-cycle", as "cycle" has come to mean 'generated by a single element', in various branches of algebra.

Henceforth, the token-set is *finite*, of cardinality $N := |\Omega|$. Further, writing the symmetric group as $\mathbb{S}_N$ shall mean that Ω is $[1\,..\,N]$ or $[0\,..\,N)$. □

Cycle-structure. Consider the following shuffle, π, of an Ace-through-King suit, Ω. Our π goes from the std order [top line], to the order in the bottom line:

A	2	3	4	5	6	7	8	9	T	J	Q	K
9	T	3	Q	A	7	4	6	5	J	K	8	2

This is called "the ***two-line*** presentation of π". [If the std token-order were understood, then just the bottom line could be shown; the ***one-line*** presentation of π.] Here, the tokens are the thirteen cards.

The ***cycle-structure*** of π is a listing of all its cycles. Note that π maps A→9→5→A; this is a 3-cycle, which I write as ⟲A 9 5⟳. [For emphasis or clarity, I might write it as ⟲A → 9 → 5⟳ or, more typically, ⟲A, 9, 5⟳.]

This *same cycle* could be written as ⟲9 5 A⟳ or as ⟲5 A 9⟳. Notice, however, that ⟲5 9 A⟳ is a <u>*different*</u> cycle; indeed, $\pi(5)$ is *not* 9.

So the ***cycle-structure*** of π is

2a: π = ⟲3⟳ ⟲A 9 5⟳ ⟲2 T J K⟳ ⟲4 Q 8 6 7⟳ .

Disjoint Cycle Notation [DCN]. In (2a), the cycles are *disjoint*; no token occurs in more than one cycle. Listing the cycles from left-to-right, first the 1-cycles [if any], then the 2-cycles, etc. is an instance of ***DCN***, ***disjoint cycle-notation***. The notation is not unique; e.g, the multiple same-length cycles could be listed in any order. Moreover, a cycle could be written starting with any of its tokens. [See CCN, below]. In DCN, if the token-set is understood, one may omit writing the 1-cycles, e.g, our (2a) could be abbreviated as

2b: π = ⟲A 9 5⟳ ⟲2 T J K⟳ ⟲4 Q 8 6 7⟳ .

However, a <u>full</u>-DCN means to list all cycles, including the 1-cycles.

Canonical Cycle Notation [CCN]. When the token set has a total-order, e.g $[1\,..\,N]$ or $\{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d}\}$, then we can use ***CCN***, ***canonical cycle-notation***:

> *i*: Write each cycle with its *largest* token first.
>
> *ii*: List cycles L-to-R with first-tokens increasing.

For example, permutation τ on ten tokens is

†:

0	1	2	3	4	5	6	7	8	9
3	8	0	4	2	7	6	5	9	1

It has four cycles; one is $(8\ 9\ 1)$; *however* CCN requires the largest token first, so we write it as $(9\ 1\ 8)$. The other cycles are (6) and $(4\ 2\ 0\ 3)$ and $(7\ 5)$. Initial tokens are $9, 6, 4, 7$; we put these in increasing order as $4<6<7<9$. Thus

‡: $$\mathsf{CCN}(\tau) \;=\; (4\ 2\ 0\ 3)\ (6)\ (7\ 5)\ (9\ 1\ 8)\,.$$

CCN requires all cycles, *including* 1-*cycles*, be listed.

What is the CCN of τ^{-1}? To invert a DCN simply reverses the order in each cycle; so *a* DCN of τ^{-1} is

$$(3\ 0\ 2\ 4)\ (6)\ (5\ 7)\ (8\ 1\ 9)\,.$$

But CCN needs each cycle to start with its largest token. So

‡‡: $$\mathsf{CCN}(\tau^{-1}) \;=\; (4\ 3\ 0\ 2)\ (6)\ (7\ 5)\ (9\ 8\ 1)\,.$$

Cycle-signature [CySig] . The ***cycle-signature*** of a permutation, lists the number of cycles of each length, from shortest to longest, with the "exponent" showing *how many* cycles of that length. For τ above, $\mathrm{CySig}(\tau) = \lceil 1^1, 2^1, 3^1, 4^1 \rfloor$. A more interesting example is perm π from (2a). $\mathrm{CySig}(\pi)$ equals

2c: $$\lceil 1^2, 3^1, 4^2 \rfloor \overset{\text{note}}{=\!=} \lceil 1^2, 2^0, 3^1, 4^2, 5^0 \ldots \rfloor\,,$$

since π has two 1-cycles, one 3-cycle, and two 4-cycles.

Each perm ν has $\mathrm{CySig}(\nu^{-1}) = \mathrm{CySig}(\nu)$.

Composing perms. In $\mathbb{S}_7$, consider $\alpha := (1\ 4\ 6\ 2\ 7)$ [omitting the 1-cycles] and $\beta := (2\ 6)(5\ 4\ 7)$. We seek to write $\alpha\beta$ [recall, our perm-composition is L-to-R] in CCN. Tracing tokens,

	$(1\ 4\ 6\ 2\ 7)$		$(2\ 6)$		$(5\ 4\ 7)$		
1	$\longmapsto$	4	$\longmapsto$	4	$\longmapsto$	7	;
7	$\longmapsto$	1	$\longmapsto$	1	$\longmapsto$	1	.
2	$\longmapsto$	7	$\longmapsto$	7	$\longmapsto$	5	;
5	$\longmapsto$	5	$\longmapsto$	5	$\longmapsto$	4	;
4	$\longmapsto$	6	$\longmapsto$	2	$\longmapsto$	2	.
3	$\longmapsto$	3	$\longmapsto$	3	$\longmapsto$	3	.
6	$\longmapsto$	2	$\longmapsto$	6	$\longmapsto$	6	.

yields a 2-cycle, 3-cycle, and two 1-cycles. Hence

$$\mathsf{CCN}(\alpha\beta) \;=\; (3)\ (5\ 4\ 2)\ (6)\ (7\ 1)\,.$$

Sign of a permutation

Several of the above concepts extend to permutations on an ∞ token-set, but the ***sign*** of a permutation is only defined for finite[♡1] permutations. For a perm β:

3: $^{\#}\mathrm{Ev}(\beta)$ *counts the # of even-length* β*-cycles.*
$^{\#}\mathrm{Od}(\beta)$ *counts the number of odd-length cycles.*
Let $^{\#}\mathrm{All}(\beta) := {}^{\#}\mathrm{Ev}(\beta) + {}^{\#}\mathrm{Od}(\beta)$.

For (2a), then, $^{\#}\mathrm{All}(\pi) = 5$ and $^{\#}\mathrm{Ev}(\pi) = 2$.

The ***sign*** of finite permutation β is

3′: $$\mathrm{Sgn}(\beta) := [-1]^{^{\#}\mathrm{Ev}(\beta)}.$$

Perm β is ***even*** [$\mathrm{Sgn}(\beta) = +1$], or ***odd*** [$\mathrm{Sgn}(\beta) = -1$], depending on whether $^{\#}\mathrm{Ev}(\beta)$ is even or odd.

A ***transposition*** is a permutation comprised of a single 2-cycle; its CySig is $\lceil 1^{[N-2]}, 2^1 \rfloor$.

> *Every permutation on a [finite] token-set is a composition*[♡2] *of transpositions.*

The goal of the section to follow, is to prove this important theorem.

4: Perm-sign thm. *For permutations* $\alpha,\beta \in \mathbb{S}_\Omega$ *on a finite token-set:* $\mathrm{Sgn}(\alpha\beta) = \mathrm{Sgn}(\alpha)\cdot\mathrm{Sgn}(\beta)$ *and* $\mathrm{Sgn}(\alpha^{-1}) = [\mathrm{Sgn}(\alpha)]^{-1} \overset{note}{=\!=} \mathrm{Sgn}(\alpha)$.

Consequently, Sgn *is a group-homomorphism from* $\big(\mathbb{S}_\Omega, \triangleright, Id_\Omega\big)$ *to* $\big(\{\pm 1\}, \cdot, 1\big)$. ◊

We'll prove this in class on Wedn., 05Oct.

[♡1] More generally, for permutations of *finite support*.

[♡2] If perm β fixes every token then β is the empty composition. Else there is a token x such that $y := \beta(x) \neq x$; so composition $\beta \triangleright \langle y, x \rangle$ fixes at least one more token than did β, hence is a composition of transpositions.