Math 222 Fall 2022, Lecture 26: Permutations

website: `https://www.cip.ifi.lmu.de/~grinberg/t/22fco`

4. Permutations

We will now revisit permutations. We have already defined and counted them, but there is a lot more to do. We will not go anywhere deep, but just introduce some of the main players and solve some of the more fundamental counting questions. Much more can be found in [Bona22], [Sagan01] and [Stanle11, Chapter 1] (see also [21s, Chapter 5] for the treatment we are mostly following here).

4.1. Basic definitions

4.1.1. Symmetric groups

> **Definition 4.1.1.** Let X be a set.
>
> **(a)** As we recall, a **permutation** of X means a bijection from X to X.
>
> **(b)** If α and β are two permutations of X, then we will denote their composition $\alpha \circ \beta$ by $\alpha\beta$.
>
> **(c)** The set of all permutations of X is denoted by S_X, and is called the **symmetric group** of X.
>
> **(d)** If $\alpha \in S_X$ and $k \in \mathbb{Z}$, then we define a permutation α^k as follows: If $k \geq 0$, then we set $\alpha^k := \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{k \text{ times}}$ (this is just standard notation for the k-th power of an arbitrary map from X to X). If $k < 0$, then we set $\alpha^k = \left(\alpha^{-1}\right)^{-k}$.

If you are familiar with abstract algebra, you will recognize that the symmetric group S_X is actually a group (with the composition operation $(\alpha, \beta) \mapsto \alpha \circ \beta$ playing the role of multiplication, and with the identity map id_X being the neutral element). This viewpoint is somewhat helpful, but not very deep; most combinatorial properties of permutations do not stem from group theory.

Note that the composition of permutations is not commutative: If α and β are two permutations in S_X, then $\alpha\beta$ usually differs from $\beta\alpha$. (There is a pretty nice formula for how often $\alpha\beta$ happens to equal $\beta\alpha$, though. See Theorem 4.3.11 in Lecture 28 below.)

Our favorite symmetric groups will be the symmetric groups $S_{[n]}$ of the sets $[n] = \{1, 2, \ldots, n\}$ for various integers $n \in \mathbb{N}$. We will discuss them so often that we introduce a shorthand for them:

Definition 4.1.2. Let $n \in \mathbb{N}$. Then, the symmetric group $S_{[n]}$ (which is the set of all permutations of $[n]$) is denoted by S_n.

As we saw in §1.7.2 (Lecture 12), if X is any n-element set, then the permutations of X can be turned into the permutations of $[n]$ by "relabelling" the elements of X as $1, 2, \ldots, n$. Thus, if we understand the symmetric groups $S_n = S_{[n]}$ for all $n \in \mathbb{N}$, then we essentially understand the symmetric groups S_X for all finite sets X (at least if we restrict ourselves to properties that don't depend on the actual elements of X). This explains why the specific symmetric groups S_n are so central to combinatorics.

4.1.2. Three notations for permutations

Definition 4.1.3. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. We introduce three notations for σ:

(a) A **two-line notation** of σ means a $2 \times n$-table $\begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ \sigma(p_1) & \sigma(p_2) & \cdots & \sigma(p_n) \end{pmatrix}$, where $p_1, p_2, \ldots, p_n$ are the elements of $[n]$ in some order. (Usually, this order is $1, 2, \ldots, n$, but sometimes a different order can make for a nicer table. Thus the indefinite article in "a two-line notation".)

(b) The **one-line notation** (short: **OLN**) of σ means the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n)) \in [n]^n$.

It is common to omit the commas and the parentheses in the OLN. So, for instance, instead of $(3, 1, 4, 2)$, you write 3142. This works fine for $n \leq 10$.

(c) The **cycle digraph** of σ is (informally) defined as a picture that is constructed as follows:

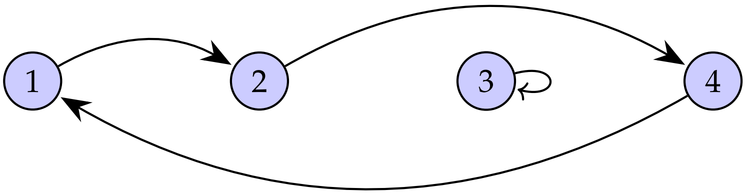
- For each $i \in [n]$, draw a point ("**node**") labelled i.
- For each $i \in [n]$, draw an arrow ("**arc**") from the node labelled i to the node labelled $\sigma(i)$.

The resulting picture is called the cycle digraph of σ. Formally speaking, it is a digraph (= directed graph[1]) with vertices $1, 2, \ldots, n$ and arcs $i \to \sigma(i)$ for all $i \in [n]$.

Example 4.1.4. Let σ be the permutation of $[4]$ whose OLN is 2431. Thus, $\sigma(1) = 2$ and $\sigma(2) = 4$ and $\sigma(3) = 3$ and $\sigma(4) = 1$. Here is one way to

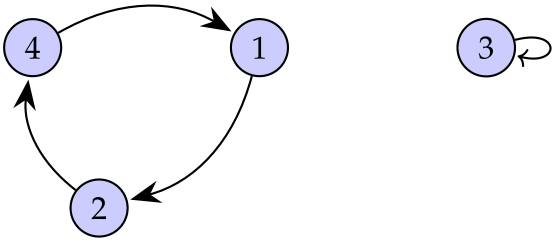
[1] For the definition (and many properties) of directed graphs, see various textbooks on graph theory, such as [ChLeZh16, Chapter 7], [Ruohon13, Chapter 3] and many others, or even my own notes [22s, Lectures 9–12]. Note that different authors use slightly different definitions, but all these definitions fit our purpose (as long as they allow loops).

draw the cycle digraph of σ:



.

Another way to draw this digraph is



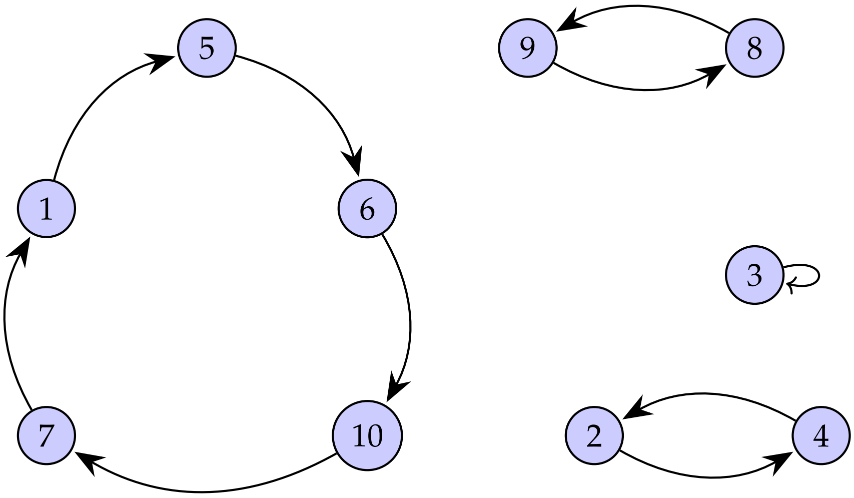
.

(When drawing cycle digraphs, one has full freedom in placing the nodes, as long as they don't overlap with the arcs. Most often, one places them in such a way that the cycles are visibly separate.)

Example 4.1.5. Let σ be the permutation of $[10]$ whose OLN is

$$5\,4\,3\,2\,6\;(10)\;1\,9\,8\,7.$$

(We have put the element 10 in parentheses to make its place clearer.) For example, $\sigma(5) = 6$ and $\sigma(6) = 10$. The cycle digraph of σ is



.

As you will have noticed from these examples, the cycle digraph of a permutation σ looks like a bunch of disjoint cycles. This is indeed the case for any permutation σ, and we will soon prove this.

The different notations for permutations have different advantages. The cycle digraph of σ is useful for understanding the "intrinsic structure" of σ, and particularly for computing powers σ^k of σ (because in order to compute $\sigma^k(i)$ for some element $i \in [n]$, we just need to start at the node labelled i, and follow the arcs for k steps). Other combinatorial properties are easier to see on the OLN.

We note that the two-line notation and the cycle digraph can be defined for any permutation σ of any finite set X (not just for $\sigma \in S_n$). The definitions are the same that we gave in Definition 4.1.3, just replacing $[n]$ by X. However, the one-line notation cannot be generalized to arbitrary finite sets X.

4.2. Transpositions and cycles

Next, we will define some important families of permutations.

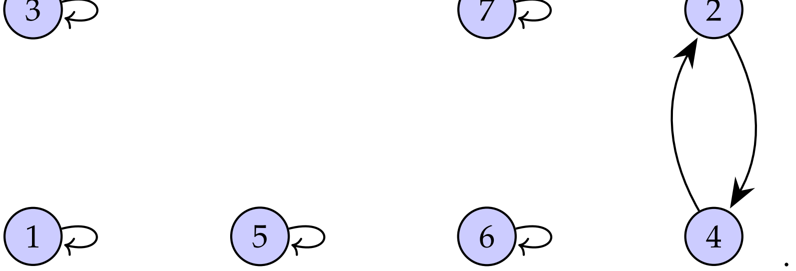
4.2.1. Transpositions

One of the simplest kinds of permutations (beyond the identity maps) are the transpositions:

Definition 4.2.1. Let X be a set. Let i and j be two distinct elements of X.

Then, the **transposition** $t_{i,j}$ is the permutation of X that sends i to j, sends j to i, and leaves all other elements of X unchanged. (We should denote this permutation by $t_{i,j,X}$, since it depends on X; but we will just call it $t_{i,j}$ because X will be clear from the context.)

Example 4.2.2. The permutation $t_{2,4}$ of the set [7] has OLN 1432567. Here is its cycle digraph:



.

More generally, any transposition $t_{i,j}$ has a cycle digraph that consists of a 2-arc cycle (containing the nodes labelled i and j) and a bunch of 1-arc cycles (each containing a single node).

Note that $t_{i,j} = t_{j,i}$ for any $i \neq j$. Thus, for an n-element set X, there are exactly $\dbinom{n}{2}$ many transpositions in the symmetric group S_X (namely, one transposition $t_{i,j}$ for every 2-element subset $\{i, j\}$ of X).

The simplest type of transpositions are the so-called simple transpositions:

Definition 4.2.3. Let $n \in \mathbb{N}$ and $i \in [n-1]$. Then, the **simple transposition** s_i is defined by

$$s_i := t_{i,i+1} \in S_n.$$

Thus, a simple transposition is a transposition that swaps two consecutive integers. The following proposition gives some basic properties of simple transpositions:[2]

Proposition 4.2.4. Let $n \in \mathbb{N}$.

(a) We have $s_i^2 = \operatorname{id}$ for each $i \in [n-1]$. More generally, $t_{i,j}^2 = \operatorname{id}$ for any $i \neq j$ in $[n]$.

(b) We have $s_i s_j = s_j s_i$ for any $i, j \in [n-1]$ satisfying $|i-j| > 1$. (This is called **transposition locality**.)

(c) We have $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} = t_{i,i+2}$ for any $i \in [n-2]$. (This is called the **braid rule**.)

Proof. Just verify that the relevant permutations send every possible input to the same output. This verification is rather straightforward. For example, in part **(c)**, we need to show that for any $i \in [n-2]$ and any $k \in [n]$, we have

$$(s_i s_{i+1} s_i)(k) = (s_{i+1} s_i s_{i+1})(k) = t_{i,i+2}(k). \tag{1}$$

This is best done by separately analyzing the four cases $k = i$, $k = i+1$, $k = i+2$ and $k \notin \{i, i+1, i+2\}$. For example, if $k = i$, then all three sides of the equality (1) equal $i+2$, whereas for $k \notin \{i, i+1, i+2\}$, they all equal k. □

4.2.2. Cycles

A more general class of permutations are the cycles, defined as follows:

Definition 4.2.5. Let X be a set. Let $i_1, i_2, \ldots, i_k$ be k distinct elements of X. Then,

$$\operatorname{cyc}_{i_1, i_2, \ldots, i_k}$$

[2] Recall that we are using the shorthand $\alpha\beta$ for the composition $\alpha \circ \beta$ of two permutations α and β.

means the permutation of X that sends

$$\begin{aligned}
&i_1 \text{ to } i_2,\\
&i_2 \text{ to } i_3,\\
&i_3 \text{ to } i_4,\\
&\ldots,\\
&i_{k-1} \text{ to } i_k,\\
&i_k \text{ to } i_1
\end{aligned}$$

and leaves all other elements of X unchanged. In other words, $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ means the permutation of X that satisfies

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k}(p) = \begin{cases} i_{j+1}, & \text{if } p = i_j \text{ for some } j \in [k]; \\ p, & \text{otherwise} \end{cases} \qquad \text{for every } p \in X,$$

where i_{k+1} means i_1.

This permutation is called a k-**cycle**.

The only 1-cycle in S_X is the identity map id_X (since $\operatorname{cyc}_i = \operatorname{id}_X$ for each $i \in X$). The 2-cycles are precisely the transpositions (since $\operatorname{cyc}_{i,j} = t_{i,j}$ for any $i \neq j$ in X).

The k-cycles have gotten their name because their cycle digraphs look as follows: one cycle of length k (containing k nodes), and all other nodes just form cycles of length 1 each. For example, the permutation σ in Example 4.1.4 is the 3-cycle $\operatorname{cyc}_{1,2,4}$.

A fairly common notation for the k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is $(i_1, i_2, \ldots, i_k)$. Many textbooks use this notation, but it requires some care, as it conflicts with the notation for the k-tuple $(i_1, i_2, \ldots, i_k)$. Thus, I use $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ instead.

The k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ does not change if we permute the k subscripts $i_1, i_2, \ldots, i_k$ cyclically:

Proposition 4.2.6. Let X be a set. For any k distinct elements $i_1, i_2, \ldots, i_k$ of X, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \operatorname{cyc}_{i_2,i_3,\ldots,i_k,i_1} = \operatorname{cyc}_{i_3,i_4,\ldots,i_k,i_1,i_2} = \cdots = \operatorname{cyc}_{i_k,i_1,i_2,\ldots,i_{k-1}}.$$

Proof. Obvious. □

Previously, we have counted the transpositions in S_X; let us now generalize this to counting k-cycles:

Exercise 1. Let $n \in \mathbb{N}$ and $k \in [n]$. Let X be an n-element set. How many k-cycles are there in S_X ?

Solution. The case $k = 1$ is easy: There is exactly one 1-cycle in S_X (for $n > 0$), since a 1-cycle is just the identity map. This should be viewed as a degenerate case; thus, we WLOG assume that $k > 1$ from now on.

Recall the notation $n^{\underline{k}}$ for the number $n(n-1)(n-2)\cdots(n-k+1)$ (this is called a falling factorial and has been introduced in Definition 2.4.2 in Lecture 7). Note that

$$n^{\underline{k}} = n(n-1)(n-2)\cdots(n-k+1) = k! \cdot \binom{n}{k} \tag{2}$$

(since $\binom{n}{k}$ is defined as $\dfrac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$).

A k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is defined for every k-tuple $(i_1, i_2, \ldots, i_k)$ of k distinct elements of X. The # of such k-tuples is easily seen to be $n^{\underline{k}}$. Indeed, we can construct such a k-tuple by first choosing its first entry i_1 (there are $|X| = n$ many options for this), then choosing its second entry i_2 (there are $n-1$ options for this, since we need i_2 to be distinct from i_1), then choosing its third entry i_3 (there are $n-2$ options for this, since we need i_3 to be distinct from both i_1 and i_2, and since i_1 and i_2 are distinct), and so on. The total # of possibilities is thus $n(n-1)(n-2)\cdots(n-k+1) = n^{\underline{k}}$.

Unfortunately, the $n^{\underline{k}}$ distinct k-tuples $(i_1, i_2, \ldots, i_k)$ do **not** produce $n^{\underline{k}}$ distinct k-cycles $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$. Indeed, Proposition 4.2.6 shows that any k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ can also be rewritten in the $k-1$ other forms

$$\operatorname{cyc}_{i_2,i_3,\ldots,i_k,i_1}, \quad \operatorname{cyc}_{i_3,i_4,\ldots,i_k,i_1,i_2}, \quad \ldots, \quad \operatorname{cyc}_{i_k,i_1,i_2,\ldots,i_{k-1}},$$

so that it is produced by k different k-tuples.

The good news is that this "ambiguity" is the worst that can happen. More precisely: A k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ always uniquely determines the elements $i_1, i_2, \ldots, i_k$ up to cyclic rotation. Indeed, if $\sigma = \operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is a k-cycle, then the elements $i_1, i_2, \ldots, i_k$ are precisely the elements of X that are not fixed by σ (it is here that we use our assumption $k > 1$), and furthermore, if we know which of these elements is i_1, then we can reconstruct the remaining elements $i_2, i_3, \ldots, i_k$ recursively by

$$i_2 = \sigma(i_1), \qquad i_3 = \sigma(i_2), \qquad i_4 = \sigma(i_3), \qquad \ldots, \qquad i_k = \sigma(i_{k-1})$$

(that is, $i_2, i_3, \ldots, i_k$ are obtained by iteratively applying σ to i_1). Therefore, if $\sigma \in S_X$ is a k-cycle, then there are precisely k different k-tuples $(i_1, i_2, \ldots, i_k)$ that satisfy $\sigma = \operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ (coming from the k options for choosing i_1 among the elements of X not fixed by σ).

In other words, for any k-cycle σ, we have

$$\left(\text{\# of } k\text{-tuples } (i_1, i_2, \ldots, i_k) \text{ of distinct elements of } X \text{ such that } \sigma = \operatorname{cyc}_{i_1, i_2, \ldots, i_k}\right)$$
$$= k. \tag{3}$$

Now, the sum rule yields

$$\begin{aligned} &(\text{\# of } k\text{-tuples } (i_1, i_2, \ldots, i_k) \text{ of distinct elements of } X) \\ &= \sum_{\substack{\sigma \in S_X \text{ is} \\ \text{a } k\text{-cycle}}} \underbrace{\left(\text{\# of } k\text{-tuples } (i_1, i_2, \ldots, i_k) \text{ of distinct elements of } X \text{ such that } \sigma = \operatorname{cyc}_{i_1, i_2, \ldots, i_k}\right)}_{\substack{=k \\ \text{(by (3))}}} \\ &= \sum_{\substack{\sigma \in S_X \text{ is} \\ \text{a } k\text{-cycle}}} k = (\text{\# of } k\text{-cycles in } S_X) \cdot k. \end{aligned}$$

Solving this for (# of k-cycles in S_X), we obtain[3]

$$\begin{aligned} &(\text{\# of } k\text{-cycles in } S_X) \\ &= \frac{1}{k} \cdot \underbrace{(\text{\# of } k\text{-tuples } (i_1, i_2, \ldots, i_k) \text{ of distinct elements of } X)}_{\substack{=n^{\underline{k}} \\ \text{(as we have seen above)}}} \\ &= \frac{1}{k} \cdot \underbrace{n^{\underline{k}}}_{\substack{=k! \cdot \binom{n}{k} \\ \text{(by (2))}}} = \underbrace{\frac{1}{k} \cdot k!}_{=(k-1)!} \cdot \binom{n}{k} = (k-1)! \cdot \binom{n}{k}. \end{aligned}$$

Thus, the general answer to Exercise 1 is

$$\begin{cases} 1, & \text{if } k = 1; \\ (k-1)! \cdot \dbinom{n}{k}, & \text{if } k > 1. \end{cases}$$

□

References

[21s] Darij Grinberg, *Algebraic Combinatorics (Drexel Spring 2021 Math 701 lecture notes)*, 4 May 2021.
`https://www.cip.ifi.lmu.de/~grinberg/t/21s/lecs.pdf`

[3] Note that we are using the shepherd's principle again.

[22s] Darij Grinberg, *Math 530: Graph Theory (Combinatorial Mathematics I), Spring 2022*.
`https://www.cip.ifi.lmu.de/~grinberg/t/22s/`

[Bona22] Miklos Bóna, *Combinatorics of Permutations*, 3rd edition, Taylor&Francis 2022.
`https://doi.org/10.1201/9780429274107`

[ChLeZh16] Gary Chartrand, Linda Lesniak, Ping Zhang, *Graphs and Digraphs*, 6th edition, CRC Press 2016.

[Ruohon13] Keijo Ruohonen, *Graph theory*, 2013.
`https://www.freetechbooks.com/graph-theory-t1080.html`

[Sagan01] Bruce Sagan, *The Symmetric Group*, Graduate Texts in Mathematics **203**, 2nd edition 2001.
`https://doi.org/10.1007/978-1-4757-6804-6`
See `https://users.math.msu.edu/users/bsagan/Books/Sym/errata.pdf` for errata.

[Stanle11] Richard P. Stanley, *Enumerative Combinatorics, volume 1*, Second edition, version of 15 July 2011. Available at `http://math.mit.edu/~rstan/ec/` .
See `http://math.mit.edu/~rstan/ec/` for errata.