0.1. A generalized principle of inclusion/exclusion

**Exercise 1.** Let $n \in \mathbb{N}$. Let $S$ be a finite set. Let $A_1, A_2, \ldots, A_n$ be finite subsets of $S$. Let $k \in \mathbb{N}$. Let $S_k$ be the set of all elements of $S$ that belong to exactly $k$ of the subsets $A_1, A_2, \ldots, A_n$. (In other words, let $S_k = \{ s \in S \mid$ the number of $i \in [n]$ satisfying $s \in A_i$ equals $k \}.$) Prove that

$$|S_k| = \sum_{I \subseteq [n]} (-1)^{|I|-k} \left( \frac{|I|}{k} \right) \left| \bigcap_{i \in I} A_i \right|. $$

Note that the principle of inclusion and exclusion (see, e.g., [Galvin17, §16]) is the particular case of Exercise 1 for $k = 0$ (since $S_0 = S \setminus \bigcup_{i=1}^n A_i$).

0.2. Summing fixed point numbers of permutations

Recall that for any $n \in \mathbb{N}$, we let $S_n$ denote the set of all permutations of $[n]$.

If $S$ is a finite set, and if $f : S \rightarrow S$ is a map, then we let $	ext{Fix } f$ denote the set of all fixed points of $f$. (That is, $	ext{Fix } f = \{ s \in S \mid f(s) = s \}.$)

**Exercise 2.** Let $n$ be a positive integer. Prove that $\sum_{w \in S_n} |\text{Fix } w| = n!$.

**[Hint: Rewrite $|\text{Fix } w|$ as $\sum_{i \in [n]} [w(i) = i]$.]**

(In other words, this exercise states that the average number of fixed points of a permutation of $[n]$ is 1.)

0.3. Transpositions $t_{i,j}$ generate permutations

Recall a basic notation regarding permutations:

**Definition 0.1.** Let $n \in \mathbb{N}$. Let $i$ and $j$ be two distinct elements of $[n]$. We let $t_{i,j}$ be the permutation in $S_n$ which switches $i$ with $j$ while leaving all other elements of $[n]$ unchanged. Such a permutation is called a transposition.

**Exercise 3.** Let $n \in \mathbb{N}$. Prove that each permutation in $S_n$ can be written as a composition of some of the transpositions $t_{1,2}, t_{1,3}, \ldots, t_{1,n}$.

(Note that this composition can be empty – in which case it is understood to be id –, and it can contain any given transposition multiple times.)
You are allowed to use the well-known fact ([Grinbe16, Exercise 5.1 (b)]) that each permutation in $S_n$ can be written as a composition of some of the transpositions $s_1, s_2, \ldots, s_{n-1}$, where $s_i$ is defined to be $t_{i,i+1}$.

0.4. V-permutations as products of cycles

Recall the following notation:

**Definition 0.2.** Let $X$ be a set. Let $k$ be a positive integer. Let $i_1, i_2, \ldots, i_k$ be $k$ distinct elements of $X$. We define $\text{cyc}_{i_1,i_2,\ldots,i_k}$ to be the permutation of $X$ that sends $i_1, i_2, \ldots, i_k$ to $i_2, i_3, \ldots, i_k, i_1$, respectively, while leaving all other elements of $X$ fixed. In other words, we define $\text{cyc}_{i_1,i_2,\ldots,i_k}$ to be the permutation of $X$ given by

$$\text{cyc}_{i_1,i_2,\ldots,i_k}(p) = \begin{cases} i_{j+1}, & \text{if } p = i_j \text{ for some } j \in \{1,2,\ldots,k\}; \\ p, & \text{otherwise} \end{cases}$$

for every $p \in X$, where $i_{k+1}$ means $i_1$.

**Exercise 4.** Let $n \in \mathbb{N}$. For each $r \in [n]$, let $c_r$ denote the permutation $\text{cyc}_{r,r−1,2,1} \in S_n$. (Thus, $c_1 = \text{cyc}_1 = \text{id}$ and $c_2 = \text{cyc}_2,1 = s_1$.) Let $G = \{g_1 < g_2 < \cdots < g_p\}$ be a subset of $[n]$. Let $\sigma \in S_n$ be the permutation $c_{g_1} \circ c_{g_2} \circ \cdots \circ c_{g_p}$.

Prove the following:

(a) We have $\sigma(1) > \sigma(2) > \cdots > \sigma(p)$.

(b) We have $\sigma([p]) = G$.

(c) We have $\sigma(p+1) < \sigma(p+2) < \cdots < \sigma(n)$.

(Note that a chain of inequalities that involves less than two numbers is considered to be vacuously true. For example, Exercise 4(c) is vacuously true when $p = n − 1$ and also when $p = n$.)

Permutations $\sigma \in S_n$ satisfying the inequalities $\sigma(1) > \sigma(2) > \cdots > \sigma(p)$ and $\sigma(p+1) < \sigma(p+2) < \cdots < \sigma(n)$ for some $p \in \{0,1,\ldots,n\}$ are known as “V-permutations” (as their plot looks somewhat like the letter “V”: first decreasing for a while, then increasing). Can you guess how permutations $\sigma \in S_n$ satisfying $\sigma(1) < \sigma(2) < \cdots < \sigma(p)$ and $\sigma(p+1) > \sigma(p+2) > \cdots > \sigma(n)$ are called?

0.5. Lexicographic comparison of permutations

**Definition 0.3.** Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ be a permutation. For any $i \in [n]$, we let $\ell_i(\sigma)$ denote the number of $j \in \{i+1, i+2, \ldots, n\}$ such that $\sigma(i) > \sigma(j)$.

For example, if $\sigma$ is the permutation of $[5]$ written in one-line notation as $[4, 1, 5, 2, 3]$, then $\ell_1(\sigma) = 3$, $\ell_2(\sigma) = 0$, $\ell_3(\sigma) = 2$, $\ell_4(\sigma) = 0$ and $\ell_5(\sigma) = 0.$
Definition 0.4. Let $n \in \mathbb{N}$. Let $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ be two $n$-tuples of integers. We say that $(a_1, a_2, \ldots, a_n) <_{\text{lex}} (b_1, b_2, \ldots, b_n)$ if and only if there exists some $k \in [n]$ such that $a_k \neq b_k$, and the smallest such $k$ satisfies $a_k < b_k$.

For example, $(4, 1, 2, 5) <_{\text{lex}} (4, 1, 3, 0)$ and $(1, 1, 0, 1) <_{\text{lex}} (2, 0, 0, 0)$. The relation $<_{\text{lex}}$ is usually pronounced “is lexicographically smaller than”; the word “lexicographic” comes from the idea that if numbers were letters, then a “word” $a_1a_2\cdots a_n$ would appear earlier in a dictionary than $b_1b_2\cdots b_n$ if and only if $(a_1, a_2, \ldots, a_n) <_{\text{lex}} (b_1, b_2, \ldots, b_n)$.

Exercise 5. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ and $\tau \in S_n$. Prove the following:
  
  (a) If $(\sigma (1), \sigma (2), \ldots, \sigma (n)) <_{\text{lex}} (\tau (1), \tau (2), \ldots, \tau (n))$, then $(\ell_1 (\sigma), \ell_2 (\sigma), \ldots, \ell_n (\sigma)) <_{\text{lex}} (\ell_1 (\tau), \ell_2 (\tau), \ldots, \ell_n (\tau))$.
  
  (b) If $(\ell_1 (\sigma), \ell_2 (\sigma), \ldots, \ell_n (\sigma)) = (\ell_1 (\tau), \ell_2 (\tau), \ldots, \ell_n (\tau))$, then $\sigma = \tau$.

0.6. Comparing subsets of $[n]$

If $I$ and $J$ are two finite sets of integers, then we write $I \leq_{\#} J$ if and only if the following two properties hold:

- We have $|I| \geq |J|$.
- For every $r \in \{1, 2, \ldots, |J|\}$, the $r$-th smallest element of $I$ is $\leq$ to the $r$-th smallest element of $J$.

For example, $\{2, 4\} \leq_{\#} \{2, 5\}$ and $\{1, 3\} \leq_{\#} \{2, 4\}$ and $\{1, 3, 5\} \leq_{\#} \{2, 4\}$. (But not $\{1, 3\} \leq_{\#} \{2, 4, 5\}$.)


  (a) For every subset $S$ of $[n]$ and every $\ell \in [n]$, let $\alpha_S (\ell)$ denote the number of all elements of $S$ that are $\leq \ell$. Prove that $I \leq_{\#} J$ holds if and only if every $\ell \in [n]$ satisfies $\alpha_I (\ell) \geq \alpha_J (\ell)$.

  (b) Prove that $I \leq_{\#} J$ if and only if $[n] \setminus J \leq_{\#} [n] \setminus I$.

Remark 0.5. Recall that we have defined a Dyck word as a list $w$ of $2n$ numbers, exactly $n$ of which are 0’s while the other $n$ are 1’s, and having the property that for each $k \in [2n]$, the number of 0’s among the first $k$ entries of $w$ is $\leq$ to the number of 1’s among the first $k$ entries of $w$.

It is not hard to see the connection between the relation $\leq_{\#}$ and Dyck words:

Let $w = (w_1, w_2, \ldots, w_{2n}) \in \{0, 1\}^{2n}$ be a list of $2n$ numbers, exactly $n$ of which are 0’s while the other $n$ are 1’s. Then, $w$ is a Dyck word if and only if

$$\{i \in [2n] \mid w_i = 1\} \leq_{\#} \{i \in [2n] \mid w_i = 0\}$$
(in other words, for every $r \in [n]$, the $r$-th appearance of 1 in $w$ precedes the $r$-th appearance of 0 in $w$).

0.7. A rigorous approach to the existence of a cycle decomposition

The purpose of the following exercise is to give a rigorous proof of the fact that any permutation can be decomposed into disjoint cycles.

Exercise 7. Let $X$ be a finite set. Let $\sigma$ be a permutation of $X$.

Define a binary relation $\sim$ on the set $X$ as follows: For two elements $x, y \in X$, we set $x \sim y$ if and only if there exists some $k \in \mathbb{N}$ such that $y = \sigma^k(x)$.

(a) Prove that $\sim$ is an equivalence relation.

For any $x \in X$, we let $[x]_{\sim}$ denote the $\sim$-equivalence class of $x$.

(b) For any $x \in X$, prove that $[x]_{\sim} = \{\sigma^0(x), \sigma^1(x), \ldots, \sigma^{k-1}(x)\}$, where $k = |[x]_{\sim}|$.

(c) For any $\sim$-equivalence class $E$, let us define $c_E$ to be the map

$$X \to X, \quad x \mapsto \begin{cases} \sigma(x), & \text{if } x \in E; \\ x, & \text{if } x \notin E. \end{cases}$$

Prove that $c_E$ is a permutation of $X$.

(d) Prove that if $E = [x]_{\sim}$ for some $x \in X$, then $c_E$ can be written as $\text{cyc}_{\sigma^0(x), \sigma^1(x), \ldots, \sigma^{k-1}(x)}$, where $k = |[x]_{\sim}|$. (Don’t forget to show that $\sigma^0(x), \sigma^1(x), \ldots, \sigma^{k-1}(x)$ are distinct, so that $\text{cyc}_{\sigma^0(x), \sigma^1(x), \ldots, \sigma^{k-1}(x)}$ is well-defined.)

(e) Let $E_1, E_2, \ldots, E_m$ be all $\sim$-equivalence classes (listed without repetitions – that is, $E_i \neq E_j$ whenever $i \neq j$). Prove that

$$\sigma = c_{E_1} \circ c_{E_2} \circ \cdots \circ c_{E_m}.$$
when the project gets updated; for a “frozen” version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2018-10-03.