2 Permutations and Subsets

Def A permutation of length n is a bijection from N_n to N_n, say $\sigma: N_n \to N_n$.
The set of all permutations of length n is denoted S_n.
Word notation. Express a permutation as $a_1 a_2 \cdots a_n$ where $a_i = \sigma(i)$.

How do we know if $a_1 \cdots a_n$ is actually word notation for a permutation?

ex 112 is not

Answer: $a_1, \ldots, a_n$ must be the numbers $1, \ldots, n$ in some order

Theorem: $\#S_n = n!$.
Informal Proof: To specify an element $a_1 \cdots a_n \in S_n$, there are n choices for a_1, $n-1$ choices for a_2, ... Therefore the total number choices is $n(n-1)\cdots 2 \cdot 1$.

Advantages	Disadvantages
- easy to understand	- doesn't appeal to principles that we established
- short and sweet	- doesn't give us an algorithm for listing all perms
	- doesn't give clues on how to generalize (generating functions)

Proof: Let $Q_n = N_n \times N_{n-1} \times \cdots \times N_2 \times N_1$. Then $\#Q_n = n(n-1)\cdots 2 \cdot 1 = n!$. We will ~~define a~~ show $S_n \rightleftarrows Q_n$ by defining an explicit bijection. This will prove that $\#S_n = \#Q_n = n!$.
Define two functions $I_n: S_n \to Q_n$ and $J_n: Q_n \to S_n$.
Function $I_n: S_n \to Q_n$.
Input: $a_1 \cdots a_n$ (a permutation in word notation)
repeat with i from 1 to n
  let $r_i = \#\{j \in \mathbb{N};\ i < j \le n \text{ and } a_i > a_j\}$.
end repeat
output $(r_1+1, \ldots, r_n+1)$

ex $\sigma = 3157642 \in S_7$
$I_7(\sigma) =$ ~~(5,6,3,1,1,1,1)~~ $(3,4,3,2,1,1)$

Check that the codomain is correct, ie if $\sigma \in S_n$ then $I_n(\sigma) \in Q_n$.
To show this we need to verify that $r_i + 1 \in N_{n+1-i}$:
$r_i + 1 \in \mathbb{N}$ because r_i is the cardinality of a finite set
$r_i + 1 \geq 1$ for the same reason
Since $\{j \in \mathbb{N};\ i < j \leq n \text{ and } a_i > a_j\} \subseteq \{j \in \mathbb{N};\ 1 < j \leq n\}$
Since $\#\{j \in \mathbb{N};\ i < j \leq n\} = n - i$, we have $r_i \leq n - i$. So $r_i + 1 \leq n - i + 1$ as required.

Function $J_n: Q_n \to S_n$
Input: $(h_1, \ldots, h_n)$
repeat with i from 1 to n
let b_i be the h_i^{th} smallest element of $N_n \setminus \{b_1, \ldots, b_{i-1}\}$
end repeat
output $b_1 \cdots b_n$

ex $\rho = (7, 1, 4, 4, 1, 2, 1) \in Q_7$.
$J_7(\rho) = 7156243$

Notes: • $b_i \neq b_j$ for any $j < i$
• since $|N_n \setminus \{b_1, \ldots, b_{i-1}\}| = n - i + 1$ and $1 \leq h_i \leq n - i + 1$: the set $N_n \setminus \{b_1, \ldots, b_{i-1}\}$ actually does have an h_i^{th} smallest element.
This shows that $b_1 \cdots b_n$ is a listing of the elements of N_n in some order, which shows that the codomain is S_n.
Finally, need to check that these are mutually inverse functions.
① $J_n(I_n(\sigma)) = \sigma$ for all $\sigma \in S_n$
② $I_n(J_n(\rho)) = \rho$ for all $\rho \in Q_n$
Verification of ①: Let $\sigma = a_1 \cdots a_n$. Write $I_n(a_1 \cdots a_n) = (r_1 + 1, \ldots, r_n + 1)$
Write $J_n(I_n(\sigma)) = J_n(r_1 + 1, \ldots, r_n + 1) = b_1 \cdots b_n$. We want to show that $a_i = b_i$ for all $i \in \{1, \ldots, n\}$. We'll prove this by strong induction.
Observation: $r_i = \#\{j \in \mathbb{N};\ i < j \leq n \text{ and } a_i > a_j\}$. This is exactly the same as saying a_i is the $(r_i + 1)^{th}$ smallest element of $\{a_i, \ldots, a_n\}$
Inductive hypothesis: Fix i, and assume that for all $1 \leq j \leq i - 1$ we have $a_j = b_j$.
Then $N_n \setminus \{b_1, \ldots, b_{i-1}\} = N_n \setminus \{a_1, \ldots, a_{i-1}\} = \{a_m, \ldots, a_n\}$. Therefore b_i is the $(r+1)^{th}$ smallest element of $\{a_i, \ldots, a_n\}$. Therefore $b_i = a_i$. This completes the strong induction. Check ② as an exercise.
This completes the proof. □

Def] Let X be a finite set. A permutation of X is a bijection $\sigma: X \to X$. Let S_X be the set of all permutations of X.

Corollary: If $\#X = n$ then $\#S_X = n!$

Proof: We show that $S_X \rightleftarrows S_n$. Since $\#X = n$, there is a bijection $f: X \to N_n$. I claim that the maps $\alpha: S_X \to S_n$, $\alpha(\sigma) = f \circ \sigma \circ f^{-1}$; $\beta: S_n \to S_X$, $\beta(\tau) = f^{-1} \circ \tau \circ f$ are mutually inverse bijections. Exercise: Verify this. □

2014 09 19

Let $\mathcal{B}(n,k)$ be the set of all k-element subsets of N_n.

ex $\mathcal{B}(4,2) = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

Theorem: $\#\mathcal{B}(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof: We'll show that

$$\mathcal{B}(n,k) \times S_k \times S_{n-k} \rightleftarrows S_n.$$

This will show that

$$\#\mathcal{B}(n,k) \cdot \#S_k \cdot \#S_{n-k} = \#S_n,$$

and hence $\#\mathcal{B}(n,k)\, k!\,(n-k)! = n!$ as desired.

To do this we define functions

$$\Psi_{n,k}: S_n \to \mathcal{B}(n,k) \times S_k \times S_{n-k}$$

and

$$\Phi_{n,k}: \mathcal{B}(n,k) \times S_k \times S_{n-k} \to S_n$$

and show they're mutually inverse.

Subroutine function: Let R_m be the set of all sequences $a_1, \ldots, a_m$ of distinct positive integers (ex $3,9,1,4,5 \in R_5$).

Function $P_m: R_m \to S_m$

Input $a_1, \ldots, a_m$

repeat with i from 1 to m

let $h_i = \#\{j \in N_m;\ a_i \geq a_j\}$

end repeat

output * $h_1, \ldots, h_m$

ex $P_5(3,9,4,1,5) = 2,5,3,1,4$

Exercise: • Verify that $P_m(a_1, \dots, a_m) \in S_m$
• Verify that if $\beta = P_m(a_1, \dots, a_m)$ then a_i is the $\beta(i)^{th}$ smallest element of $\{a_1, \dots, a_m\}$.

Function: $\Psi_{n,k} : S_n \to \mathcal{B}(n,k) \times S_n \times S_{n-k}$
Input $a_1 \cdots a_n$
Let $A = \{a_1, \dots, a_k\}$
$\beta = P_k(a_1 \cdots a_k)$
$\gamma = P_{n-k}(a_{k+1} \cdots a_n)$
Output (A, β, γ)

ex $\Psi_{7,4}(3,6,7,1,4,5,2) = (\{1,3,6,7\}; 2,3,4,1; 2,3,1)$

Function $\Phi_{n,k} : \mathcal{B}(n,k) \times S_k \times S_{n-k} \to S_n$
Input: (A, β, γ)
Sort A as $s_1 < \cdots < s_k$
Sort $N_n \setminus A$ as $t_1 < \cdots < t_{n-k}$
repeat with i from 1 to k
let $c_i = s_{\beta(i)}$
end repeat
repeat with j from 1 to $n-k$
let $c_{k+j} = t_{\gamma(j)}$
end repeat
output $c_1 \cdots c_n$

Final step of proof: Show that:
① $\Phi_{n,k}(\Psi_{n,k}(\sigma)) = \sigma \quad \forall \sigma \in S_n$
② $\Psi_{n,k}(\Phi_{n,k}((A,\beta,\gamma))) = (A,\beta,\gamma) \quad \forall (A,\beta,\gamma) \in \mathcal{B}(n,k) \times S_k \times S_{n-k}$
Verification of ①.
Write $\sigma = a_1 \cdots a_n$ in word notation.
$\Psi_{n,k}(\sigma) = (A, \beta, \gamma)$
$\Phi_{n,k}(\Psi_{n,k}(\sigma)) = c_1 \cdots c_n$
Goal: Show $a_i = c_i$ $\forall i \in [n]$.
Then $A = \{a_1, \dots, a_k\}$, $\beta = P_k(a_1 \cdots a_k)$, $\gamma = P_{n-k}(a_{k+1} \cdots a_n)$
We observed earlier that a_i is the $\beta(i)^{th}$ smallest element of A.

In the algorithm for $\mathcal{I}_{n,k}$, $c_i = s_{a(i)}$ which is the $a(i)^{th}$ smallest element of A. $\therefore a_i = c_i$ for $i \in \{1, \ldots, k\}$.
Similarly, c_{k+j} is the $f(j)^{th}$ smallest element of $N_n \setminus A = \{a_{k+1}, \ldots, a_n\}$ and so is a_{k+j}. $\therefore c_{k+j} = a_{k+j}$ for $j = 1, \ldots, n-k$.
Combining the two arguments $a_i = c_i$ for $i \in \{1, \ldots, n\}$.
Verification of ②: Exercise.
① and ② show that we have the required bijections and the result follows. ∎

For an arbitrary finite set X, define $\mathcal{B}(X,k)$ to be the set of all k-element subsets of X.

Corollary: If $\#X = n$, then $\#\mathcal{B}(X,k) = \binom{n}{k}$.
Proof: Exercise.

Binomial Theorem

$$(1+y_1)\cdots(1+y_n) = \sum_{S \subseteq N_n} y^S$$

Set $y_1 = \cdots = y_n = x$, LHS $\to (1+x)^n$, ~~RHS $\to \sum_{S \subseteq N_n} x^{\#S}$~~

$$\text{RHS} \to \sum_{S \subseteq N_n} x^{\#S} = \sum_{k=0}^{n} \sum_{S \subseteq N_n,\, \#S = k} x^{\#S}$$

$$= \sum_{k=0}^{n} \sum_{S \subseteq N_n,\, \#S = k} x^k$$

$$= \sum_{k=0}^{n} x^k \sum_{S \subseteq N_n;\, \#S = k} 1$$

$$= \sum_{k=0}^{n} x^k \sum_{S \in \mathcal{B}(n,k)} 1$$

$$= \sum_{k=0}^{n} x^k \, \#\mathcal{B}(n,k)$$

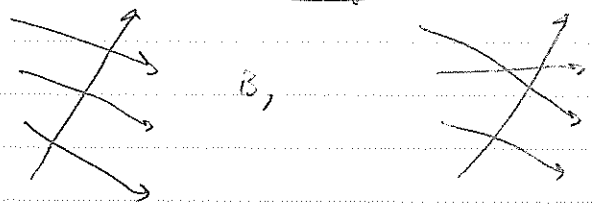
$$= \sum_{k=0}^{n} \binom{n}{k} x^k .$$

eyglrdk?

2014 09 22

A permutation $\sigma \in S_n$ a <u>derangement</u> is $\sigma(i) \neq i$ for all $i \in N_n$.

ex



Let $D_n \subseteq S_n$ denote the set of all derangements of length n. What is $\#D_n$?
To answer this, use inclusion-exclusion.
Define $A_i = \{\sigma \in S_n ; \sigma(i) = i\}$. Then $D_n = S_n \setminus (A_1 \cup \cdots \cup A_n)$.
For any $\emptyset \subset S \subseteq N_n$, $\sigma \in S_n$ is in A_S if and only if $\sigma(i) = i \ \forall i \in S$.
If $\#S = k$, we're fixing k values for σ, and the rest get permuted.
$\therefore \#A_S = \#$ of permutations of $N_n \setminus S = (n-k)!$

$$\therefore \#(A_1 \cup \cdots \cup A_n) = \sum_{\emptyset \subset S \subseteq N_n} (-1)^{\#S-1} \#A_S$$

$$= \sum_{k=1}^{n} \sum_{S \in \mathcal{B}(n,k)} (-1)^{\#S-1} \#A_S$$

$$= \sum_{k=1}^{n} \sum_{S \in \mathcal{B}(n,k)} (-1)^{k-1} (n-k)!$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)!$$

$$= n! \sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k!}$$

$$\therefore \#D_n = \#S_n - \#(A_1 \cup \cdots \cup A_n)$$

$$= n! - n! \sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

As $n \to \infty$,

$$\frac{\#D_n}{n!} \to \frac{1}{e},$$

the probability that a random permutation is a derangement.