Random Permutations

Application in

- Encryption of digital images

- Low density parity check (LDPC) codes

Definition of Permutation: A permutation of the set $\{1, 2, 3, ..., n\}$ is a 1-1 function g from $\{1, 2, 3, ..., n\}$ onto itself

$$g : \{1, 2, 3, ..., n\} \rightarrow \{1, 2, 3, ..., n\}$$

Example: $\{1, 2, 3, 4, 5\} \rightarrow \{4, 1, 3, 5, 2\}$

Number of Fix Points in a Random Permutation

Assume that all the possible permutations are equally likely. Since there are $n!$ possible permutations, the probability of any given one is

$$\frac{1}{n!}$$

A fix point in a permutation g is point i for which

$$g(i) = i$$

In the example above we have

$$\begin{aligned} g(1) &= 4 \\ g(2) &= 1 \\ \mathbf{g(3) = 3} &\quad \text{fix point} \\ g(4) &= 5 \\ g(5) &= 2 \end{aligned}$$

Let

$$A_i = \{i \text{ is a fix point}\}$$

Then

$$P(A_i) = \frac{(n-1)!}{n!} = \frac{1}{n}, \quad 1 \le i \le n,$$

$$P(A_i \cap A_j) = \frac{(n-2)!}{n!} = \frac{1}{n(n-1)}, \quad 1 \le i < j \le n,$$

etc.

Problem: Calculate the probability of zero fix points in a random permutation.

Solution

As before, let

$$A_i = \{i \text{ is a fix point}\}$$

and

$$B_n^0 = \{\text{there are zero fix points}\}$$

Then

$$B_n^0 = (\cup_{i=1}^n A_i)^c$$

$$P\left(B_n^0\right) = P\left[(\cup_{i=1}^n A_i)^c\right] = 1 - P\left(\cup_{i=1}^n A_i\right)$$

$$= 1 - \sum_{j=1}^{n} (-1)^{j-1} \sum_{|J_n|=j} P\left(\cap_{i \in J_n} A_i\right) \quad \text{(inclusion-exclusion)}$$

Moreover

$$\sum_{|J_n|=j} P\left(\cap_{i \in J_n} A_i\right) = \binom{n}{j} \frac{(n-j)!}{n!} = \frac{n!\,(n-j)!}{(n-j)!j!n!} = \frac{1}{j!}$$

For example,

$$\sum_{|J_n|=1} P\left(\cap_{i\in J_n} A_i\right) = P\left(A_1\right) + P\left(A_2\right) + \cdots + P\left(A_n\right) = \left(\begin{array}{c} n \\ \\ 1 \end{array} \right) P\left(A_1\right) = n\frac{(n-1)!}{n!} = 1,$$

$$\sum_{|J_n|=2} P\left(\cap_{i\in J_n} A_i\right) = P\left(A_1 \cap A_2\right) + \cdots + P\left(A_{(n-1)} \cap A_n\right) = \left(\begin{array}{c} n \\ \\ 2 \end{array} \right) P\left(A_1 \cap A_2\right) = \left(\begin{array}{c} n \\ \\ 2 \end{array} \right) \frac{(n-2)!}{n!} = \frac{1}{2},$$

etc.

Therefore

$$P\left(B_n^0\right) = 1 - \sum_{j=1}^{n} (-1)^{j-1} \frac{1}{j!} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^{n-1} \frac{1}{n!}$$

$$= \sum_{j=0}^{n} (-1)^{j} \frac{1}{j!} \approx e^{-1}$$

n	$P\left(B_n^0\right)$
1	0.0000000
2	0.5000000
3	0.3333333
4	0.3750000
5	0.3666667
6	0.3680556

n	$P\left(B_n^0\right)$
7	0.3678571
8	0.3678819
9	0.3678792
10	0.3678795
$\vdots$	$\vdots$
∞	0.3678794

Problem: Calculate the probability of $1 < k \leq n$ fix points in a random permutation.

Solution

Given k numbers from the set $\{1, 2, 3, ..., n\}$, the probability that they are the only fix points is

$$\frac{(n-k)!}{n!} P\left(B_{n-k}^{0}\right) = \frac{1}{n\left(n-1\right)\cdots\left(n-k+1\right)} P\left(B_{n-k}^{0}\right)$$

Note: this is intuitively clear and can be formalized using conditional probabilities. For example, let $n = 5$ and calculate the probability that 1 and 2 are the only fix points in a random permutation. Set

$$R = \{1 \text{ and } 2 \text{ are the only fix points}\}$$
$$A = \{1 \text{ and } 2 \text{ are fix points}\}$$
$$B = \{3, 4 \text{ and } 5 \text{ are not fix points}\}$$

Then

$$R = A \cap B$$
$$P\left(R\right) = P\left(A \cap B\right) = P\left(A\right) P\left(B|A\right) = \frac{2!}{5!} P\left(B_{3}^{0}\right)$$

Since the k numbers can be chosen in $\left(\begin{array}{c} n \\ k \end{array} \right)$, we have

$$P\left(B_{n}^{k}\right) = \left(\begin{array}{c} n \\ k \end{array} \right) \frac{1}{n\left(n-1\right)\cdots\left(n-k+1\right)} P\left(B_{n-k}^{0}\right)$$

$$= \frac{n!}{k!\left(n-k\right)!} \frac{(n-k)!}{n!} P\left(B_{n-k}^{0}\right) = \frac{1}{k!} P\left(B_{n-k}^{0}\right)$$

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

NOTE: Naturally, we take $P\left(B_0^0\right) = 1$.

Numerical Calculation: let's take $n = 10$ to calculate $P\left(B_n^k\right)$ for $k = 0, 1, 2, ..., 10$.

k	$P\left(B_{10}^k\right)$
0	0.3678795
1	0.3678792
2	0.183 94
3	0.06131
4	0.015336
5	0.0030556
6	0.00052083
7	0.000066138
8	0.000012401
9	0.0000000
10	0.00000027557