Mathematical Foundations of Computer Science

This Lecture: Combinatorics - Derangements

Department of Mathematical and Computational Sciences
National Institute of Technology Karnataka, Surathkal

MA714 (Odd Semester [2025-26])

Introduction

The derangement problem is a classical problem in combinatorics. It asks how many permutations of n elements exist in which none of the elements appear in their original positions. Such permutations are called "**derangements**" or "**complete permutations**".

Definition 1

*A **derangement** is a permutation σ of the set $\{1, 2, \cdots, n\}$ such that $\sigma(i) \neq i$ for all i. The number of derangements of a set of n elements is denoted by $D(n)$.*

Recollect the Maclaurin's series for the exponential function:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

In particular, $e^{-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots$.

$e^{-1}0.36788$ upto 5 decimal places and $\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots \approx$ 0.36786.

This means that for all $k \in \mathbb{Z}^+$, if $k \geq 7$, then $\sum_{n=0}^{k} \frac{x^n}{n!}$ is a very good approximation to e^{-1}.

Example 1

The number of derangements of $1, 2, 3, 4$ *is*
$D(4) = 4![1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!}] = 9.$

These 9 derangements are

$$\begin{array}{ccc} 2143 & 3142 & 4123 \\ 2341 & 3412 & 4312 \\ 2413 & 3421 & 4321 \end{array}$$

Example 2

Mahesh, the editor of Sujatha Publishers, has 7 books to be reviewed before their publication. He requests 7 people to review them. The usual practice is that two reviews are obtained for each book. So, the first week he gives each reviewer one book to read and then redistributes those books in the second week. In how many ways can he make these two distributions so that he obtains two reviews (by different reviewers) for each book?

Solution: Mahesh can distribute the books in $7!$ ways in the first week. Let us number both the books and the reviewers (for the first week) as $1, 2, 3, 4, 5, 6, 7$. Then Mahesh has to redistribute the books in the second week so that none of the reviewers gets the same book again. Obviously, this can be done in $D(7)$ ways. Now, by the rule of product, he can make the two distributions in $(7!)D(7) = (7!)^2(e^{-1})$ ways.

Example 3

During a horse race, Shashi bets on each of the 10 horses in the race to come in according to how they are favoured. In how many ways can the horses reach the finish line so that Shashi loses all his bets?
Solution: Evidently, horses and racetrack have no much importance in this problem! We want to know in how many ways we can arrange the numbers $1, 2, \cdots, 10$ *so that no number sits in its place in the increasing order, which means, this is clearly a derangements problem.*
PIE provides the key to calculate this. For each $1 \leq i \leq 10$*, an arrangement of* $1, 2, \cdots, 10$ *is said to satisfy the condition* c_i *if the integer i is in the* i^{th} *place. Then we obtain the number of derangements as*

Example 3 (contd...)

$D(10) = N(\overline{c}_1\overline{c}_2\cdots\overline{c}_{10})$
$= 10! - \binom{10}{1}9! + \binom{10}{2}8! - \binom{10}{3}7! + \cdots + (-1)^{10}\binom{10}{10}0!$
$= 10![1 - \binom{10}{1}\frac{9!}{10!} + \binom{10}{2}\frac{8!}{10!} + \cdots + \binom{10}{10}\frac{0!}{10!}]$
$= 10![1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{10!}] \approx (10!)e^{-1}.$

Remark 1

Since there are $10!$ *ways of horses reaching the finishing line, the probability that Shashi will lose every bet is approximately* $\frac{(10!)e^{-1}}{(10!)} = e^{-1}$.

1. **Cryptography**: Derangements are used in certain key-generation algorithms to avoid fixed points, improving security.
2. **Testing and Fault Tolerance**: Derangements model test scenarios where responses or test results are randomly reassigned to avoid bias.
3. **Hashing Algorithms**: Hash functions often use derangements to ensure a uniform and non-repetitive distribution.
4. **Secure Shuffling**: In secure multiparty computation, derangements help in simulating fair and unbiased shuffling mechanisms.
5. **Scheduling Problems**: Derangements apply to task assignment problems where no task can be assigned to its original agent.

Summary

The derangement problem provides deep insights into permutations and has practical applications in many areas of Computer Science. Its connection with inclusion-exclusion principle, recurrence relations, and combinatorial identities makes it a rich topic for study.

Suggested References

1. Kenneth Rosen, *Discrete Mathematics and its Applications*, 5^{th} edition, McGraw Hill, NY, 2003.
2. C.L. Liu, Elements of Discrete Mathematics, 2^{nd} edition, McGraw Hill.