Mathematics for Computer Science

TD5

October 8th, 2025

Question. *Prove that the number of derangement of order n is*

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

Before proving the result, let us just recall that for all set X, we note $\mathfrak{S}(X)$ the *set of permutation of* X, that is to say the set of all bijections $f : X \to X$. For convenience, we write $\mathfrak{S}_n \overset{\text{def}}{=} \mathfrak{S}\left(\llbracket n \rrbracket\right)$. We will state and prove two lemmas before showing the main result.

Lemma 1. *Let $n \in \mathbb{N}$, $n \geq 3$. Then D_n verifies the following property:*

$$D_n = (n-1)\left(D_{n-2} + D_{n-1}\right).$$

Proof. Let $n \geq 3$. Suppose that n people have each brought a gift. The gifts are then mixed up so that each person is given an item that they did not bring. We are going to count how many different ways this can be done. We observe that person number 1 must choose a gift among the set $k \in \llbracket 2, n \rrbracket$ and we note for the sake of argument that there are $\binom{n-1}{1} = n-1$ ways to do this. The person numbered k (*i.e.* the one who brought gift number k), must also choose a gift. We then distinguish between two cases, for which we will count the number of possible derangements.

▷ Suppose that person k takes the gift number 1. Now, we want to count the number of valid derangement in this situation, *i.e.* we want to count the number of bijection $\sigma : \llbracket n \rrbracket \to \llbracket n \rrbracket$ with no fixed point such that $\sigma(1) = k$ and $\sigma(k) = 1$. Since the values for the images of 1 and k are given, we have to find a valid derangement for the remaining people $\llbracket n \rrbracket \setminus \{1, k\}$, that is to say a valid derangement for the remaining $n-2$ people. By definition, there is exactly D_{n-2} ways to perform such permutation.

▷ Suppose that person k takes anything but the gift number 1. Let $\tau = \begin{pmatrix} 1 & k \end{pmatrix}$ be the permutation that exchanges 1 and k. Let us define two sets:

$$\mathcal{A} = \left\{ \sigma \in \mathfrak{S}_n \;\middle|\; \begin{array}{l} \sigma \text{ has no fixed points ;} \\ \sigma(1) = k \text{ and } \sigma(k) \neq 1 \end{array} \right\} \qquad \text{and} \qquad \mathcal{B} = \left\{ \gamma \in \mathfrak{S}\left(\llbracket 2, n \rrbracket\right) \,\middle|\, \gamma \text{ has no fixed points} \right\}$$

and we show that $\mathcal{A}$ and $\mathcal{B}$ are in bijection.

↱ If we take $\sigma \in \mathcal{A}$, we observe that $\tau \circ \sigma$ is a bijection $\llbracket n \rrbracket \to \llbracket n \rrbracket$ that has exactly one fixed point: 1. Indeed, let us compute the image of every element by distinguishing between three different cases:

- Image of 1: $(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(k) = 1$.
- Image of $\sigma^{-1}(1)$: since $\sigma(k) \neq 1$, and we have $\sigma^{-1}(1) \neq k$ $(\tau \circ \sigma)\left(\sigma^{-1}(1)\right) = \tau(1) = k \neq \sigma^{-1}(1)$.
- Otherwise, we take $j \in \llbracket n \rrbracket \setminus \left\{1, \sigma^{-1}(1)\right\}$. Then $\sigma(j) \neq 1$ and $\sigma(j) \neq k$, therefore $(\tau \circ \sigma)(j) = \tau\left(\sigma(j)\right) = \sigma(j)$. Since σ has no fixed-points $(\tau \circ \sigma)(j) \neq j$.

If we consider $\gamma \overset{\text{def}}{=} (\tau \circ \sigma)_{|\llbracket 2,n \rrbracket}$ the restriction of $\tau \circ \sigma$ on $\llbracket 2, n \rrbracket$, we have that γ is a bijection that has no fixed-point, thus $\gamma \in \mathcal{B}$. It means that the application $f : \sigma \in \mathcal{A} \mapsto (\tau \circ \sigma)_{|\llbracket 2,n \rrbracket} \in \mathcal{B}$ is well defined.

↱ Conversly, if $\gamma \in \mathcal{B}$ is a bijection $\llbracket 2, n \rrbracket \to \llbracket 2, n \rrbracket$ with no fixed-point, then γ can be extended to a bijection $\overline{\gamma} \in \mathfrak{S}_n$ by setting $\overline{\gamma}(j) = \gamma(j)$ for all $j \in \llbracket 2, n \rrbracket$, and $\overline{\gamma}(1) = 1$. Considering $\sigma \overset{\text{def}}{=} \tau \circ \overline{\gamma}$, we have:

- Image of 1: $\sigma(1) = \tau \circ \overline{\gamma}(1) = \tau(1) = k$.
- Image of k: $\sigma(k) = \tau \circ \overline{\gamma}(k)$. Since $\overline{\gamma}(k) = \gamma(k) \notin \{1, k\} = \mathrm{Supp}(\tau)$, $\sigma(k) = \gamma(k) \neq 1$. Moreover, $\sigma(k) = \gamma(k) \neq k$.
- Moreover, let us show that σ has no fixed-point. Suppose that $j \in \llbracket n \rrbracket$ is a fixed-point, that is to say an element such that $\sigma(j) = j$, and we seek for a contradiction. From a previous analysis, we know that $j \notin \{1, k\}$. It implies that $j = \tau(j) = \overline{\gamma}(j) = \gamma(j)$, wich contradicts $\gamma \in \mathcal{B}$. Thus, σ cannot have any fixed point.

Therefore, $\sigma \in \mathcal{A}$, and the application $g : \gamma \in \mathcal{B} \mapsto \tau \circ \overline{\gamma} \in \mathcal{A}$ is well defined.

Now, we will show that $g \circ f = \mathrm{id}_{\mathcal{A}}$. By definition, $g \circ f$ takes a permutation $\sigma \in \mathcal{A}$, and performs several changes to σ: first, the application of f swiches the images of 1 and k, then removes the mapping $1 \mapsto 1$. Then, the appliction of g reintroduice the mapping $1 \mapsto 1$, and swiches back the images of 1 and k. Overall, the permutation σ is left unchanged, therefore $g \circ f = \mathrm{id}_{\mathcal{A}}$

Conversly, we want to show that $f \circ g = \mathrm{id}_{\mathcal{B}}$. For all $\gamma \in \mathcal{B}$, the application of g extends γ with the mapping $1 \mapsto 1$, and then swiches the images of 1 and k. Then the application of f swiches back the images of 1 and k, before removing the mapping $1 \mapsto 1$. Overall, $f \circ g$ left γ unchanged, thus $f \circ g = \mathrm{id}_{\mathcal{B}}$.

Finally, f and g are two mapping wich are reciprocal one of another, thus f and g are bijections. It gives $\mathcal{A} \simeq \mathcal{B}$, and in particular those two sets have the same cardinal. Thus, the number of valid derangement in the case where people 1 takes gift k and person k doesn't take present 1 is equal to the cardinal of $\mathcal{B}$ wich is exactly the number of derangement of a set of $n-1$ elements: we have $|\mathcal{A}| = |\mathcal{B}| = D_{n-1}$.

Finally, there is in total $D_{n-2} + D_{n-1}$ ways to perform a derangement of the set $[\![n]\!]$ such that 1 takes present k. Since there is $n-1$ possibilities for the value of k, the final number of derangement of a set of n elements verifies

$$D_n = (n-1)\left(D_{n-2} + D_{n-1}\right).$$

□

From this, we will deduce easely the following result:

Lemma 2. *For any $n \in \mathbb{N}$, $n \geq 2$, $D_n = nD_{n-1} + (-1)^n$.*

Proof. We will show the result by induction on n.

▷ *Base case* : for $n = 2$, we have $D_2 = 1 = 2 \times \underbrace{D_1}_{=0} + (-1)^2$.

▷ *Induction step* : let $n \in \mathbb{N}$, $n \geq 3$ such that the wanted identity is true at rank $n-1$, *i.e.* $D_{n-1} = (n-1)D_{n-2} + (-1)^{n-1}$. Since $n \geq 3$, we will be able to use the identity from **lemma 1**. We then compute:

$$\begin{aligned} D_n - nD_{n-1} - (-1)^n &= (n-1)\left(D_{n-2} + D_{n-1}\right) - nD_{n-1}\underbrace{-(-1)^n}_{=(-1)^{n-1}} && \text{(by \textbf{lemma 1})} \\ &= (n-1)D_{n-2} - D_{n-1} + (-1)^{n-1} \\ &= 0. && \text{(by induction hypothesis)} \end{aligned}$$

Therefore, $D_n = nD_{n-1} + (-1)^n$, the wanted identity is thus true at rank n.

▷ *Conclusion* : by induction principle, we have for all $n \geq 2$ that $D_n = nD_{n-1} + (-1)^n$.

□

We are now ready to show the main result:

Proof. We will show by induction on $n \in \mathbb{N}^*$ that

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

▷ *Base case* : for $n = 1$, we have $D_1 = 0 = \frac{1}{0!} - \frac{1}{1!}$.

▷ *Induction step* : let $n \geq 2$ such that

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

We deduce from **lemma 2** that

$$D_n = nD_{n-1} + (-1)^n = \underbrace{n(n-1)!}_{=n!} \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} + n! \cdot \frac{(-1)^n}{n!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

▷ *Conclusion* : by induction principle, the wanted closed formula for D_n is established.

□