Mathematics for Computer Science

TD2

September 17^{th}, 2025

Question. *Write below the closed formula for $J(n)$ and its complete formal proof.*

Let us recall some intermediate results on $J(n)$:

Lemma 1. *For all $n \in \mathbb{N}^*$, we have*

$$J(2n) = 2J(n) - 1 \qquad (\spadesuit)$$
$$J(2n+1) = 2J(n) + 1. \qquad (\heartsuit)$$

Proof. Let $n \in \mathbb{N}^*$. Suppose $2n$ people are standing in a circle and start killing each other according to the rebels' rules. After n kills, all the people with even numbers are dead and only the people with odd numbers remain, meaning there are exactly n people left. Moreover, at this stage, the first person has to kill next, so we know that the surviving person is the $J(n)^{\text{th}}$ person standing in the reduced circle. This person is labelled the $J(n)^{\text{th}}$ odd number, which is $2J(n) - 1$. According to the definition of the Josephus number, the person who survives in a group of $2n$ people is $J(2n)$, which is $2J(n) - 1$, giving us identity ($\spadesuit$).

A similar argument can be used to show the other identity: suppose $2n+1$ people are standing. After n kills, everyone with an even number is dead. For the $(n+1)^{\text{th}}$ kill, the person labelled $2n+1$ kills number 1: there are now n people left standing, and these are exactly the odd numbers except for 1. We know that the surviving person is the $J(n)^{\text{th}}$ person standing in the reduced circle. This person is labelled the $(J(n)+1)^{\text{th}}$ odd number (since the first odd number, 1, is already dead), which is $2J(n)+1$. According to the definition of the Josephus number, the person who survives in a group of $2n+1$ people is $J(2n+1)$, which is $2J(n)+1$, proving identity ($\heartsuit$). □

We are now ready to establish a closed formula for Josephus number.

Proof. We will prove by induction that:

$$\forall k \in \mathbb{N}, \quad \forall i \in [\![0, 2^k - 1]\!], J\left(2^k + i\right) = 2i + 1.$$

▷ *Base case* : at $k \stackrel{\text{def}}{=} 0$, the set $[\![0, 2^k - 1]\!]$ is reduced at $\{0\}$. Therefore, we only have one case to check: $i \stackrel{\text{def}}{=} 0$. We have

$$J\left(2^k + i\right) = J\left(2^0 + 0\right) = J(1) = 1 = 2 \cdot 0 + 1 = 2i + 1$$

so, for the base case $k \stackrel{\text{def}}{=} 0$, we have shown that for any $i \in [\![0, 2^k - 1]\!]$, $J\left(2^k + i\right) = 2i + 1$.

▷ *Induction step* : let $k \in N$ be such that for any $j \in [\![0, 2^k - 1]\!]$, $J\left(2^k + j\right) = 2j + 1$. To show the induction step, we will have to show that for any $i \in [\![0, 2^{k+1} - 1]\!]$, $J\left(2^{k+1} + i\right) = 2i + 1$. Thus, we take $i \in [\![0, 2^{k+1} - 1]\!]$. We can then distinguish between two cases:

- *If i si even* : we write $i = 2m$ for some $m \in \mathbb{N}$. In particular, by assumption on i we have $0 \le 2m \le 2^{k+1}$, thus $m \in [\![0, 2^k - 1]\!]$. We then have:

$$\begin{aligned}
J\left(2^{k+1} + i\right) &= J\left(2\left(2^k + m\right)\right) \\
&= 2J\left(2^k + m\right) - 1 && \text{(by } \textbf{Lemma 1}\text{, identity } (\spadesuit)) \\
&= 2(2m+1) - 1 && \text{(by induction hypothesis and the fact that } 0 \le m \le 2^k - 1) \\
&= 2i + 1.
\end{aligned}$$

- *If i si odd* : we write $i = 2m+1$ for some $m \in \mathbb{N}$. In particular, by assumption on i we have $0 \leq 2m+1 \leq 2^{k+1}$, thus $m \in \left[\!\left[0, 2^k - 1\right]\!\right]$. We then have:

$$\begin{aligned} J\left(2^{k+1} + i\right) &= J\left(2\left(2^k + m\right) + 1\right) \\ &= 2J\left(2^k + m\right) + 1 && \text{(by \textbf{Lemma 1}, identity ($\heartsuit$))} \\ &= 2(2m+1) + 1 && \text{(by induction hypothesis and the fact that } 0 \leq m \leq 2^k - 1) \\ &= 2i + 1. \end{aligned}$$

In both cases, we have shown that $J\left(2^{k+1} + i\right) = 2i + 1$ for any $i \in \left[\!\left[0, 2^{k+1} - 1\right]\!\right]$, which means that our induction hypothesis holds at rank $k+1$.

▹ *Conclusion* : by induction principle, we have that

$$\forall k \in \mathbb{N}, \quad \forall i \in \left[\!\left[0, 2^k - 1\right]\!\right], J\left(2^k + i\right) = 2i + 1.$$

In particular, for all $n \in \mathbb{N}^*$, we can write n as $n = 2^r + \ell$, in such way that 2^r is the *largest possible power of two that fits in n* and $\ell \in [\![0, 2^r - 1]\!]$. Applying the result shown by induction, we have

$$J(n) = J\left(2^r + \ell\right) = 2\ell + 1.$$

□

Remarks.

▹ *By the definition we gave of r as being the only natural number such that $2^r \leq n < 2^{r+1}$, we have that r is the unique natural number satisfying*

$$r \leq \log_2(n) < r + 1$$

thus, $r = \lfloor \log_2(n) \rfloor$. This property gives also an expression for ℓ:

$$\ell = n - 2^{\lfloor \log_2(n) \rfloor}$$

and therefore we can express $J(n)$ as:

$$J(n) = 2\left(n - 2^{\lfloor \log_2(n) \rfloor}\right) + 1.$$

▹ *If n is a number written in base 2,*

$$n = (1\underbrace{\alpha_{r-1}\alpha_{r-2}\cdots\alpha_1\alpha_0}_{\text{sequence of 0's and 1's}})_{\text{base 2}} \qquad \textit{and we have} \qquad J(n) = (\underbrace{\alpha_{r-1}\alpha_{r-2}\cdots\alpha_1\alpha_0}_{\text{same } r \text{ lats bits of } n}1)_{\text{base 2}}.$$

Indeed, the number defined by the sequence $(\alpha_{r-1}\alpha_{r-2}\cdots\alpha_1\alpha_0)_{\text{base2}}$ is exaclty what remains of n when we have removed the largest power of 2 (represented by the first bit of n), therefore $(\alpha_{r-1}\alpha_{r-2}\cdots\alpha_1\alpha_0)_{\text{base2}} = \ell$. Computing the n^{th} Josephus number involves the base two representation of ℓ by two and adding one. This is exactly the same as putting a one at the end of the base two representation of ℓ.