JOSEPHUS PROBLEM

Denis TRYSTRAM

Lecture notes **Maths for Computer Science** – *MOSIG 1 – 2018*

1 Josephus' problem

The problem comes from an old story reported by Flavius Josephus during the Jewish-Roman war in the first century. The legend reports that Flavius was among a band of 41 rebels trapped in a cave by the roman army. Preferring suicide to capture, the rebels decided to form a circle and proceeding around to kill every second remaining person until no one was left. As Josephus had some skills in Maths and wanted none of this suicide non-sense, he quickly calculated where he should stand in the circle in order to stay alive at the end of the process.

Definition. Given n successive numbers in a circle. The problem is to determine the *survival number* (denoted by $J(n)$) in the process of removing every second remaining number starting from 1 (see figure 1).

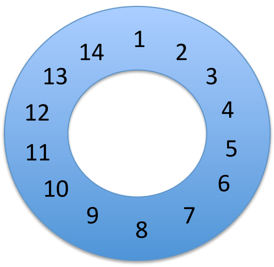

Figure 1: Initial situation for the Josephus process.

In particular, we are going to determine if there exists a closed formula. Guessing the answer sounds not obvious. We need to better understand the progression.

Property 1. $J(n)$ is odd
Proof. This is straightforward since the first tour removes all even numbers! See figure 2.

We called *round*, the set of steps to come back at a given position in the circle. Starting at 1, the first round is completed after $\lceil \frac{n}{2} \rceil$ steps. Then, again half of the of the remaining numbers are removed in the second round and so on.

How many rounds do we have for determining $J(n)$? If N denotes this number, it verifies $\Sigma_{i=1}^{i=N} \frac{1}{2^i} = 1$.

Property 2. (even numbers) $J(2n) = 2J(n) - 1$

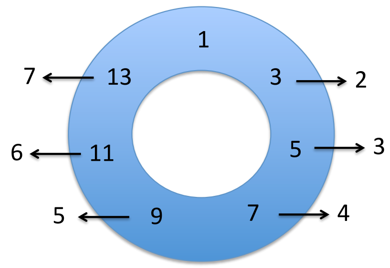

Figure 2: First step of the process (n is even).

Proof. This is a simple generalization of the previous property. If n is even, the first round corresponds simply to come back to the original circle where one half of the points have been removed.

From this, we deduce $J(2^m) = 1$ for all m.
Let us turn to odd numbers.

Property 3. (odd numbers) $J(2n + 1) = 2J(n) + 1$

We can compute easily the first ranks. It turns out that the progression is composed of grouped terms starting at each power of 2. Let $n = 2^m + k$, the rule within each group m is to start at 1 and increase by 2 the successive numbers $(0 \leq k < 2^m)$. Let prove it by recurrence on n.

Property 4. $J(2^m + k) = 2k + 1$
Proof.

- **Basis.** $n = 1$, thus $m = 0$, $k = 0$ and $J(1) = 2^0 + 0 = 1$
- **Induction step.** Suppose the formula holds for any integer lower than $n = 2^m + k$. Since there are two expressions for $J(.)$, we distinguish the cases whether k is even and k is odd:
  - If k is even, then, $2^m + k$ is even, and we can write:
    $J(2^m + k) = 2J(2^{m-1} + \frac{k}{2}) - 1$
    by induction hypothesis, $J(2^{m-1} + \frac{k}{2}) = 2\frac{k}{2} + 1 = k + 1$
    Thus, $J(2^m + k) = 2(k + 1) - 1 = 2k + 1$.
  - If k is odd, the proof is similar:
    $J(2^m + k) = 2J(2^{m-1} + \lfloor \frac{k}{2} \rfloor) + 1 = 2\lfloor \frac{k}{2} \rfloor + 1 = 2k + 1$.

We can even go one step further with this problem by remarking that powers of 2 play an important role. Let us use the radix 2 representation of n and $J(n)$:

$n = \sum_{j=0}^{j=m} b_j.2^j = b_m.2^m + b_{m-1}.2^{m-1} + ... + b_1.2 + b_0$

$n = (1b_{m-1}...b_1b_0)_2$ since by definition of m $b_m = 1$

$k = (0b_{m-1}...b_1b_0)_2$ since $k < 2^m$

Thus, using the closed formula for $J(n)$:

$J(n) = (b_{m-1}...b_0b_m)_2$.

In other words, the solution is obtained by a simple shift of the binary representation of n. Applied to $n = 41 = (101001)_2$ Josephus Flavius was able to determine the last position in few seconds: $(010011)_2 = 19$.