
A Proof of Elmsley's Binary Translocation No. 1

The Collected Works of Alex Elmsley, Volume 2, Page 311.

Let $b \in \mathbb{N}$.

Definition. Let $k \in \mathbb{N}$. Define $f_k : \mathbb{N} \rightarrow \mathbb{N}$ by

$$f_k(x) := bx - b + 1 + k, \quad \forall x \in \mathbb{N}.$$

Theorem. Let $n \in \mathbb{N}$. Write $n - 1$ in b -ary form: $n - 1 = \sum_{i=0}^m c_i b^i$, where $m \in \mathbb{N}$ and $c_i \in \{0, 1, \dots, b - 1\} \forall 0 \leq i \leq m$. Then

$$n = f_{c_0} f_{c_1} \cdots f_{c_m}(1).$$

Proof. By induction on m we will show that $1 + \sum_{i=0}^m c_i b^i = f_{c_0} \cdots f_{c_m}(1)$, which is equivalent to the assertion.

For $m = 0$ we have $f_{c_0}(1) = b - b + 1 + c_0 = 1 + c_0$. Now suppose the formula holds up to $m - 1$. Thus - by shifting the index numbering - we have the induction hypothesis $f_{c_1} \cdots f_{c_m}(1) = 1 + \sum_{i=1}^m c_i b^{i-1}$. By applying f_{c_0} we get $f_{c_0}(1 + \sum_{i=1}^m c_i b^{i-1}) = b \cdot (1 + \sum_{i=1}^m c_i b^{i-1}) - b + 1 + c_0 = b + \sum_{i=1}^m c_i b^i - b + 1 + c_0 = 1 + \sum_{i=0}^m c_i b^i$. \square

Corollary. From the above Theorem, Elmsley's application immediately follows for $b := 2$. This is seen as follows. The top card should be faroed to the n -th position from the top of the deck, thus $n - 1$ has to be expressed in 2-ary (i.e. binary) form. In this case we have $c_i \in \{0, 1\}$ and f_1 acts like an in-faro and f_0 like an out-faro, since $\forall x \in \mathbb{N}$ (where x represents a position in the deck, counting from the top):

$$c_i = 0 : f_{c_i}(x) = f_0(x) = 2x - 1$$

$$c_i = 1 : f_{c_i}(x) = f_1(x) = 2x.$$

So the expression $f_{c_0} f_{c_1} \cdots f_{c_m}(1)$ describes indeed the journey of the top card when the shuffles are performed according to the binary pattern of $n - 1$.

(Note that in a deck with a finite number of cards (those are quite common), these formulas are only true if x represents a position in the upper half of the deck. In this application f_{c_i} is never applied to a position in the lower half by construction, since n cannot be greater than the number of cards. Therefore the binary form of $n - 1$ cannot have enough digits to cause problems, as can easily be verified.)