

## An exercise from “The Art of Computer Programming”

In page 89 of the book “The Art of Computer Programming (Volume 1)”, Donald Knuth presents an interesting identity used to extract every  $m^{\text{th}}$  term of a series. Let  $\omega$  be an  $m^{\text{th}}$  root of unity (that is,  $\omega^m = 1$ ) and  $0 \leq r < m$ ; we have

$$(0) \quad \langle \Sigma n : n \bmod m = r : g.n \times z^n \rangle = \frac{1}{m} \times \langle \Sigma k : 0 \leq k < m : \omega^{-k \times r} \times G.(\omega^k \times z) \rangle .$$

In the same page he points out to exercise 14, which asks the reader to prove (0). The solution given in the book directs the reader to the solution of a different problem which, in my opinion, is quite cryptic. I wrote this note to record my solution, which is a straightforward verification of (0).

In the following text,  $R.z$  denotes the right-hand side of (0) and the function  $[z^n]$  yields the  $n^{\text{th}}$  coefficient of the generating function it receives as argument.

### Verifying the identity

We want to prove that  $[z^n] R.z$  is  $g.n$  when  $n \bmod m = r$ , and 0 otherwise. So, considering the integer division of  $n$  by  $m$ , we suppose that  $n = q \times m + x$ , with  $0 \leq x < m$ . With this assumption, the goal is to prove that the  $[z^n] R.z$  is  $g.n$  when  $x = r$ , and 0 otherwise. We calculate as follows:

$$\begin{aligned} & [z^n] R.z \\ = & \quad \{ \quad R.z \text{ is the right-hand side of (0)} \quad \} \\ & [z^n] \left( \frac{1}{m} \times \langle \Sigma k : 0 \leq k < m : \omega^{-k \times r} \times G.(\omega^k \times z) \rangle \right) \\ = & \quad \{ \quad \text{scalar multiplication and } [z^n] \text{ distributes over addition} \quad \} \\ & \frac{1}{m} \times \langle \Sigma k : 0 \leq k < m : \omega^{-k \times r} \times [z^n] G.(\omega^k \times z) \rangle \\ = & \quad \{ \quad [z^n] G.(c \times z) = c^n \times [z^n] G.z \quad \text{with } c := \omega^k \quad \} \\ & \frac{1}{m} \times \langle \Sigma k : 0 \leq k < m : \omega^{-k \times r} \times \omega^{k \times n} \times g.n \rangle \\ = & \quad \{ \quad n = q \times m + x \text{ and arithmetic} \quad \} \\ & \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : \omega^{k \times (q \times m + x - r)} \rangle \\ = & \quad \{ \quad \omega^{k \times q \times m} = 1 \quad \} \\ & \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : \omega^{k \times (x - r)} \rangle . \end{aligned}$$

Now we have two cases:  $x = r$  and  $x \neq r$ . If  $x = r$ , then:

$$\begin{aligned}
& \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : \omega^{k \times (x - r)} \rangle \\
= & \{ \quad x = r \quad \} \\
& \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : 1 \rangle \\
= & \{ \quad \text{evaluate the sum} \quad \} \\
& \frac{1}{m} \times g.n \times m \\
= & \{ \quad \text{arithmetic} \quad \} \\
& g.n .
\end{aligned}$$

If  $x \neq r$ , we have:

$$\begin{aligned}
& \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : \omega^{k \times (x - r)} \rangle \\
= & \{ \quad \text{arithmetic} \quad \} \\
& \frac{1}{m} \times g.n \times \langle \Sigma k : 0 \leq k < m : (\omega^{(x - r)})^k \rangle \\
= & \{ \quad \text{geometric progression} \quad \} \\
& \frac{1}{m} \times g.n \times \frac{1 - (\omega^{(x - r)})^m}{1 - \omega^{(x - r)}} \\
= & \{ \quad \omega^{m \times (x - r)} = 1 \quad \} \\
& \frac{1}{m} \times g.n \times \frac{0}{1 - \omega^{(x - r)}} \\
= & \{ \quad \text{arithmetic} \quad \} \\
& 0 .
\end{aligned}$$

We conclude that

$$\begin{aligned}
& \text{if } n \bmod m = r \rightarrow [z^n] R.z = g.n \\
& \square \quad n \bmod m \neq r \rightarrow [z^n] R.z = 0 \\
& \text{fi,}
\end{aligned}$$

which means that (0) is valid.

João Fernando Ferreira  
February 28, 2008

School of Computer Science, University of Nottingham  
NG8 1BB, UK  
joao@joaoferreira.org