Problem

A ***permutation*** on the set {1, . . . , k} is a one-to-one, onto function on this set. When p is a permutation, p^t means the composition of p with itself t times. Let

$$PERM\text{-}POWER = \{\langle p, q, t\rangle \mid p = q^t \text{ where } p \text{ and } q \text{ are permutations on } \{1, \ldots, k\} \text{ and } t \text{ is a binary integer}\}.$$

Show that *PERM-POWER* ? P. (Note that the most obvious algorithm doesn't run within polynomial time. Hint: First try it where t is a power of 2.)

Step-by-step solution

Step 1 of 2

A permutation on the set $\{1,\ 2,\ \ldots,\ k\}$ is a one-to-one, onto function on this set. If *p* is a permutation then p^t says that the composition of *p* with itself t times.

The PERM-POWER is defined as follows:

$$\begin{aligned}\text{PERM-POWER} = \{< p,\ q,\ t > \mid p = q^t \text{ where } p \text{ and } q \text{ are permutations on } \{1,\ldots,k\}\\ \text{and } t \text{ is a binary integer}\}\end{aligned}$$

Comment

Step 2 of 2

The binary integer *t* can be represented as $t = x_0 2^0 + x_1 2^1 + \ldots + x_n 2^n$ where x_i acquires a value either 0 or 1.

Now, q^t can be written as,

$$\begin{aligned} q^t &= q^{x_0 2^0 + x_1 2^1 + \ldots + x_n 2^n} \\ &= q^{x_0 2^0} \times q^{x_1 2^1} \times \ldots \times q^{x_n 2^n} \end{aligned}$$

From this, compute q^{2^j} where $j = 1,\ 2, \ldots,\ \lfloor \log t \rfloor$. By substituting *j* value, q^{2^j} can be $q^1,\ q^2,\ q^4,\ q^8,\ \cdots$. It is easy to compute the permutation by applying *q* on *q* itself. It takes $O(k \log t)$ steps to compute q^{2^j} where each product requires $O(k)$ steps. Finally, the value of q^{2^j} is compared with *p* which takes additional *k* steps. Thus, it can be said that $\text{PERM-POWER} \in \text{P}$.

Comment