Random Number Generation without Repetition
Jayadev Misra
3/27/96

Problem: We are given a function f from naturals to naturals. Let f^i denote the i-fold application of f to a fixed argument, f^0.

Theorem: $(\exists i,t : i \geq 0 \wedge t > 0 : (f^i = f^{i+t}) \Rightarrow (\exists j : i \leq j < i+t : f^j = f^{2j}))$

Proof: Consider the interval of numbers i through $i+t-1$. Since this interval contains t numbers, there exists j, $i \leq j < i+t$, which is a multiple of t. Since $f^i = f^{i+t}$ and j is a multiple of t, $f^k = f^{k+j}$, for all k, $k \geq i$. Letting k be j, $f^j = f^{2j}$.

Corollary: $(\forall j : m \leq j < n : f^j \neq f^{2j}) \Rightarrow (\forall i,k : m \leq i < k \leq n : f^i \neq f^k)$

Proof: We prove the contrapositive of this result.

$$
\begin{array}{ll}
 & (\exists i,k : m \leq i < k \leq n : f^i = f^k) \\
\Rightarrow & \quad \{ \text{ From Theorem, using the introduced values } i,k \text{ } \} \\
 & (\exists j : i \leq j < k : f^j = f^{2j}) \\
\Rightarrow & \quad \{ \text{ relaxing the bounds on } j \text{ } \} \\
 & (\exists j : m \leq j < n : f^j = f^{2j})
\end{array}
$$

Note: This is an interesting example where a producer has two produce two items, f^{2j-1} and f^{2j}, and the consumer can then consume a single item, f^j, provided $f^j \neq f^{2j}$.