Homework N

Joe Baker, Brett Schreiber, Brian Knotten

March 20, 2018

42

43

Assume that $f^k(x)$ is not a one-way permutation of x. $f^k(x)$ is still a permutation, since $f(x)$ is a permutation. So therefore $f^k(x)$ is not one-way. That means an algorithm A could figure out the input in polynomial time.

Construct an algorithm B as follows:
Given x and the one-way permutation f:
    Run A on f, x to get y such that $f^k(y) = x$.
    Repeat the following procedure $k - 1$ times:
        $y' := f(y)$
        $y := y'$
    Return y'

Since k is polynomial on n, then B is a polynomial algorithm, since it loops only $k - 1$ times. B returns the final value y' such that $f(y') = x$. Therefore B can reverse f. But f is a one way permutation. It cannot be cracked in polynomial time. There is a contradiction. Therefore f^k must also be a one-way permutation.