Pseudo-random Generator

To make a psedo-random-generator, we take the Discrete Logarithm Problem (DLP) as one-way function (owf) denoted by f.
DLP: Given p, g and $f(x) = g^x \ (mod\, p)$, $\forall$ Probabilistic Polynomial-time Turing Machine (PPTM) A, it is computationally infeasible for A to find a y such that $f(x) = f(y)$.

$$P[A(1^n, f(x)) = y, f(x) = f(y)] \leq negl(n)$$

where security parameter $n = |x|$ and $negl(n)$ is a negligible function.
We take the hardcore predicate of DLP as $h(x) = MSB(x)$. From the definition of hardcore predicate, $\forall$ PPTM A,

$$P[A(1^n, f(x)) = h(x)] \leq \frac{1}{2} + negl(n)$$

This means that the hardcore predicate bit cannot be distinguished from a random bit with probability negligibly more than $\frac{1}{2}$.

Let's define $G : \{0,1\}^n \to \{0,1\}^{n+1}$ to be $G(x) = f(x)||h(x)$ (DLP output appended to MSB of input). We see that G is a pseudo-random

generator (PRG) because if we assume $\exists$ PPTM A such that,

$$|P[A(U_{n+1}) = 1] - P[A(G(U_n)) = 1]| > negl(n)$$

This means that the probability of distinguishing G's output from a truly random generator is greater than $negl(n)$ which implies that the probability of finding the $MSB(x)$ is greater than $\frac{1}{2}$.

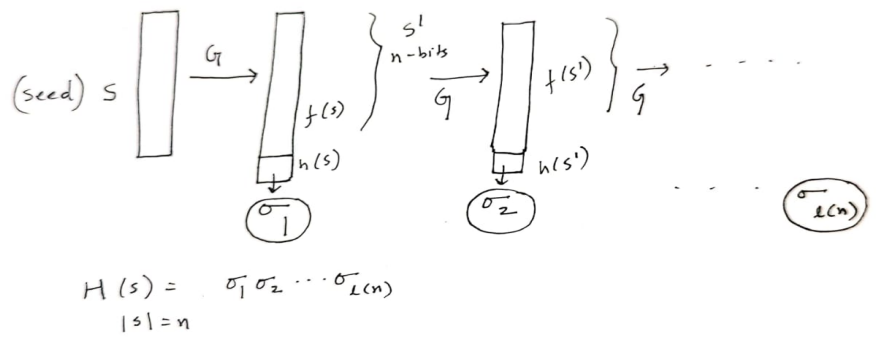
$$P[A(f(x)) = h(x)] > \frac{1}{2} + negl(n)$$

But, if $h(x)$ is a hardcore predicate of $f(x)$, $\forall$ PPTM A,

$$P[A(f(x)) = h(x)] \leq \frac{1}{2} + negl(n)$$

leading to contradiction. Hence, $G(x)$ is a PRG.

We now devise a PRG $H : \{0,1\}^n \to \{0,1\}^{l(n)}$ from PRG $G : \{0,1\}^n \to \{0,1\}^{n+1}$ for polynomial $l(n)$.
Let us define H as follows:



If H is not a PRG, we should be able to distinguish sequence generated by H from a truly random sequence $r_1 r_2 \dots r_{l(n)}$. Consider the following sequences,

$\sigma_1 \sigma_2 \sigma_3 \dots \sigma_{l(n)}$

$r_1 \sigma_2 \sigma_3 \dots \sigma_{l(n)}$

$r_1 r_2 \sigma_3 \dots \sigma_{l(n)}$

$\vdots$

$r_1 r_2 \dots r_{l(n)}$

Any two consecutive sequences in this list differ in one element. Since we can distinguish between the first and last sequence, we can distinguish between any two sequences from this list and consequently, any two consecutive sequences as well.

This implies that we can distinguish r_i from σ_i where $i \in \{1, 2, \dots l(n)\}$.This contradicts the pseudo-randomness of PRG G. Hence, H is a PRG.