pseudorandom generator

Canonical name	PseudorandomGenerator
Date of creation	2013-03-22 13:03:16
Last modified on	2013-03-22 13:03:16
Owner	Henry (455)
Last modified by	Henry (455)
Numerical id	6
Author	Henry (455)
Entry type	Definition
Classification	msc 68Q30
Defines	stretch function

Let G be a deterministic polynomial-time function from $\mathbb{N}^{<\omega}$ to $\mathbb{N}^{<\omega}$ with *stretch function* $l : \mathbb{N} \to \mathbb{N}$, so that if x has length n then $G(x)$ has length $l(n)$. Then let G_n be the distribution on strings of length $l(n)$ defined by the output of G on a randomly selected string of length n selected by the uniform distribution.

Then we say G is *pseudorandom generator* if $\{G_n\}_{n\in\mathbb{N}}$ is pseudorandom.

In effect, G translates a random input of length n to a pseudorandom output of length $l(n)$. Assuming $l(n) > n$, this expands a random sequence (and can be applied multiple times, since G_n can be replaced by the distribution of $G(G(x))$).