- If $f(n)$ is negligible, $\sqrt{f(n)}$ is negl.

Let $p(n)$ be an arbitrary poly.

To prove: There exists a N s.t

$\exists$

for all $n > N$, $\sqrt{f(n)} < \frac{1}{p(n)}$

$f(n) < \frac{1}{p^2(n)}$ (use $f(n)$ is negl.) ← change of vars

← if $p(n)$ is poly, so is $p^2(n)$

so $\exists N$, s.t $n > N$ $\underbrace{f(n) < \frac{1}{p^2(n)}}_{f(n) \text{ is negl.}}$ or $\sqrt{f(n)} < \frac{1}{p(n)}$

$$G(s) = \underbrace{s \overset{\text{concat}}{\cdot} \underbrace{1010\cdots}_{n \text{ bits}}}$$

Is G a PRG?

$\ell(n) = 2n > n$

world 0

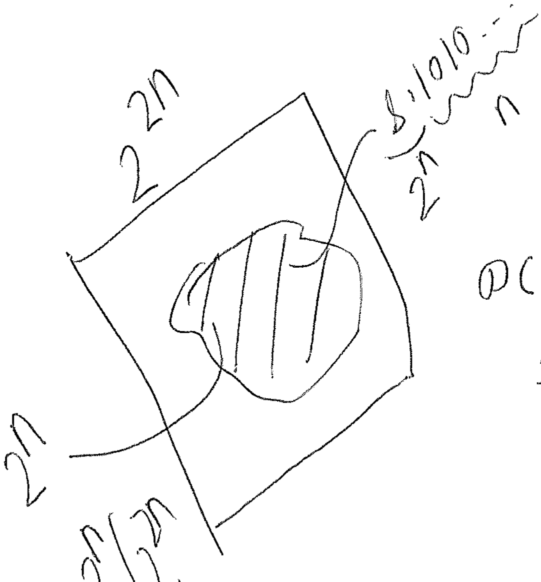
$s \leftarrow \{0,1\}^n$

$r = G(s)$

give r to D

PRG

$P[D(G(s))=1] = 1$



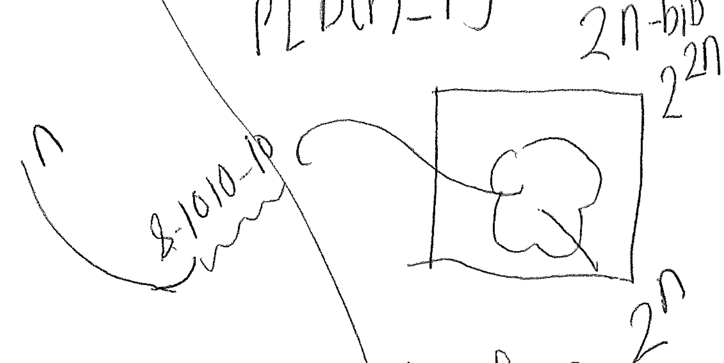
world 1

$r \leftarrow \{0,1\}^{2n}$

give r to D

~~PRG~~
random

$P[D(r)=1] = \frac{2^n}{2^{2n}} = 2^{-n}$



$$\underset{\substack{\uparrow \\ 2n \text{ bits}}}{D(w)} = \begin{cases} 1 & w \text{ of the form } s \cdot 10\cdots \\ 0 & \text{otherwise} \end{cases}$$

$1 - 2^{-n} \neq$ negl.

$$2^{-100 \log n} \leftarrow \text{base 2}$$

$$\|$$

$$\left(2^{-\log n}\right)^{100} = \frac{1}{n^{100}} \neq \text{negl.}$$

$$\frac{1}{n^{100}} < \frac{1}{n^{200}}$$

$$\frac{1}{2^{\sqrt{n}} + n^{1000} + n^4} < \frac{1}{2^{\sqrt{n}}}$$

$$\uparrow \text{negl.} \qquad \uparrow \text{negl.}$$

$$\underbrace{\frac{n^2+n}{2^n}}_{\text{negl.}} + \underbrace{\frac{n^3+n^4}{2^{\sqrt{n}}}}_{\text{negl.}} = \text{negl.}$$

$\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$

n

$\mathcal{A}$

1^n $\qquad$ 1^n

$k \leftarrow \mathrm{Gen}(1^n)$ $\longleftarrow$ m_0, m_1

$|m_0| = |m_1|$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathrm{Enc}_k(m_b)$ $\longrightarrow$

guess b'

$$\text{output} = \begin{cases} 1 & b = b' \\ 0 & b \neq b' \end{cases}$$

PPT

$$\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$$

*

$$\Pr[\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$$