5 Prove that $f(s): \{0,1\}^n \to \{0,1\}^n$ OWP
$h(s): \{0,1\}^n \to \{0,1\}$ HARD-CORE PREDICATE

PRG $G(s) = f(s) \| h(s)$ is secure

[2]: P. 269

THEOREM 7.6 *Let f be a one-way permutation and let* hc *be a hard-core predicate of f. Then, $G(s) \stackrel{\text{def}}{=} f(s) \| \mathsf{hc}(s)$ is a pseudorandom generator with expansion factor $\ell(n) = n + 1$.*

Theorem 5. OWP with a HC bit $\Rightarrow$ PRG.

Proof. Let $f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a OWP, and let $h : \{0,1\}^\lambda \to \{0,1\}$ be its HC bit. We claim that $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ where $G(x) = (f(x), h(x))$ is a PRG.

Assume that G is not a PRG. Then, there exists a PPT A such that

$$|\underbrace{Pr_{x \xleftarrow{\$} \{0,1\}^\lambda}[1 \leftarrow A(G(x))]}_{\text{GAME}} - \underbrace{Pr_{y \xleftarrow{\$} \{0,1\}^{\lambda+s(\lambda)}}[1 \leftarrow A(y)]}_{\text{HYB}'}| \geq \varepsilon(\lambda)$$

(A can distinguish between PRG output and a RANDOM string of same length

where ε is non-negligible. Note that

$$Pr_{y \xleftarrow{\$} \{0,1\}^{\lambda+s(\lambda)}}[1 \leftarrow A(y)] = \underbrace{Pr_{x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}}[1 \leftarrow A(f(x), b)]}_{\text{HYB}''}$$

f(x) is uniformly distributed when x is uniform

since f is a permutation, so we have

$$|Pr_{x \xleftarrow{\$} \{0,1\}^\lambda}[1 \leftarrow A(f(x), h(x))] - Pr_{x \xleftarrow{\$} \{0,1\}^\lambda, b \xleftarrow{\$} \{0,1\}}[1 \leftarrow A(f(x), b)]| \geq \varepsilon(\lambda).$$

This directly contradicts the definition of a HC bit. Thus, G must be a PRG. □

$\text{GAME}_{A,G}(1^\lambda)$

$A(1^\lambda)$		$C(1^\lambda)$	HYB'	HYB''
		$x \leftarrow \$ \{0,1\}^\lambda$		$b \leftarrow \$ \{0,1\}$
	$\xleftarrow{z}$	$z = G(x)$	$z \leftarrow \$ \{0,1\}^{\lambda+1}$ ($s(\lambda)$)	$z = f(x) \| b$
	$\xrightarrow{b'}$	$= f(x) \| h(x)$		

for $G(x)$ to be a SECURE PRG we have

$$\{ GAME^{PRG}_{\mathcal{A},G}(1^\lambda) \} \approx_c \{ HYB'(1^\lambda) \}$$

and that

$$\{ HYB'(1^\lambda) \} = \{ HYB''(1^\lambda) \}$$ because $f(x)$ OWP

so truly uniformly distributed

By CONTRADICTION we assume $\exists$ PPT $\mathcal{A}$ which breaks PRG security (distinguish with $Pr >$ negl between GAME and HYB' <u>and so between GAME and HYB''</u>), then we can build $\mathcal{A}'$ by REDUCTION which breaks HC $h(x)$

$\mathcal{A}$		$\mathcal{A}'$		$\mathcal{C}_{HC}$
				$x \leftarrow \{0,1\}^\lambda$
				$f(x)$ OWP
			$\xleftarrow{(f(x),\, b)}$	b: $h(x)$ HC or $U_1 \in \{0,1\}$
	$\xleftarrow{z}$	$z = f(x) \Vert b$		
	$\xrightarrow{b'}$		$\xrightarrow{b'}$	

if $b = h(x)$ z is distributed like $G(x)$ in GAME, if $b = U_1$ z has the same distribution as in HYB' so in HYB''

$\mathcal{A}$ w.p $>$ negl(λ) can distinguish between $z = G(x) = f(x) \Vert h(x)$ and $z = f(x) \Vert b = U_n$ and with the same $Pr >$ negl(λ) $\mathcal{A}$ can distinguish between $(f(x), h(x))$ and $(f(x), U_1)$

$$\Longrightarrow (f(x), h(x)) \not\approx_c (f(x), U_1)$$

$$\Longrightarrow h(x) \text{ NOT HC for } f(x)$$

$$\Longrightarrow G \text{ must be a PRG}$$