Exercise (Existence of hard-core bits). A predicate $\pi : S \rightarrow \{0,1\}$ is said to be a $\varepsilon$-regular if the output distribution for uniform input distribution is nearly uniform:

$$\Delta(\pi) = |\Pr[s \leftarrow S : \pi(s) = 0] - \Pr[s \leftarrow S : \pi(s) = 1]| \leq \varepsilon .$$

A predicate $\pi$ is a $(t,\varepsilon)$-unpredictable also known as $(t,\varepsilon)$-hardcore predicate for a function $f : S \rightarrow X$ if for any $t$-time adversary $\text{Adv}_{hc-pred}^{f,\pi}(A) = 2 \cdot |\Pr[s \leftarrow S : A(f(s)) = \pi(s)] - \frac{1}{2}| \leq \varepsilon .$

Prove that any $(t,\varepsilon)$-hardcore predicate is $2\varepsilon$-regular. Let $f : S \rightarrow \{0,1\}^n$ be a deterministic function and let $\pi_k(s)$ denote the $k$th bit of $f(s)$ and $f_k(s)$ denote the output of $f(s)$ without the $k$th bit. Show that if $f$ is a $(t,\varepsilon)$-secure pseudorandom generator, then $\pi_k$ is $(t,\varepsilon)$-hardcore predicate for $f_k$.

Solution. Regularity. As the first step, we first unroll the game inlined into the probability formula that defines advantage against hard-core predicates:

$$\begin{align*}
G & \left[ 
s \leftarrow S \\
 x \leftarrow f(s) \\
 b \leftarrow \pi(s) \\
 \text{return} \ [b = A(x)] .
\end{align*}$$

This representation highlights that $A$ must choose between two complex hypotheses $[\pi(s) = 0]$ and $[\pi(s) = 1]$. If one of these hypotheses is significantly more probable than the other, then the adversary $A_*$ abuse this fact and output the most probable hypothesis without looking at the input. Let

$$\begin{align*}
\alpha_0 &= \Pr[s \leftarrow S : \pi(s) = 0] \\
\alpha_1 &= \Pr[s \leftarrow S : \pi(s) = 1]
\end{align*}$$

the corresponding probabilities for hypotheses. Then it is straightforward to see that

$$\text{Adv}_{hc-pred}^{f,\pi}(A_*) = |\alpha_0 - \frac{1}{2}| = |\alpha_1 - \frac{1}{2}| = \frac{1}{2} \cdot |\alpha_0 - \alpha_1|$$

$$= \frac{1}{2} \cdot |\Pr[s \leftarrow S : \pi(s) = 0] - \Pr[s \leftarrow S : \pi(s) = 1]| .$$

Consequently, any predicate that is not $2\varepsilon$-regular can be predicted without looking at the input with advantage at least $\varepsilon$. Thus, the first claim is proved.

Indistinguishability. Although the definition of hard-core predicate is given through a single guessing game, we can represent it also in terms of indistinguishability. Let us first define two sets:

$$\begin{align*}
S_0 &= \{s \in S : \pi(s) = 0\} \\
S_1 &= \{s \in S : \pi(s) = 1\} .
\end{align*}$$

Then we can define following distinguishing games:

$$\begin{align*}
G_0 & \left[ 
s \leftarrow S_0 \\
x \leftarrow f(s) \\
\text{return} \ A(x)
\right]
\end{align*} \quad \begin{align*}
G_1 & \left[ 
s \leftarrow S_1 \\
x \leftarrow f(s) \\
\text{return} \ A(x)
\right]
\end{align*}$$

1
If the sizes of sets are equal $|S_0| = |S_1|$, then the game $G$ can be thought as simple guessing between equiprobable seed distributions $S_0$ and $S_1$ and thus

$$\text{Adv}^\text{hc-pred}_{f,\pi}(A) = |\Pr [G^A_0 = 1] - \Pr [G^A_1 = 1]| .$$

In general, the probability of seed distributions $S_0$ and $S_1$ is slightly off balance and thus

$$|\Pr [G^A_0 = 1] - \Pr [G^A_1 = 1]| = 2 \cdot |\Pr [s \epsilon S: A(f(s)) = \pi(s)] - \max \{\alpha_0, \alpha_1\}| \leq 2 \cdot |\Pr [s \epsilon S: A(f(s)) = \pi(s)] - \frac{1}{2}| + 2 \cdot |\alpha_0 - \frac{1}{2}| \leq \text{Adv}^\text{hc-pred}_{f,\pi}(A) + 2 \cdot \Delta(\pi) .$$

Consequently, we could define hard-core predicates in terms of indistinguishability games as long as we require that the predicate is nearly regular. For regular predicates, these two notions coincide.

**Analysis of a standard construction.** Let $k$ be fixed and let $x_\bullet$ denote a bitstring $x_n \ldots x_{k+1}x_{k-1}x_1$ that is obtained by dropping the $k$th bit from $n$-bit string $x = x_n \ldots x_1$. To show that $\pi_k$ is an hardcore bit, we have to analyse the following game:

$$G_0 \begin{cases} s \epsilon S \\ x \epsilon f(s) \\ \text{return } [x_k \not= A(x_\bullet)] . \end{cases}$$

By our assumption $f(s)$ is indistinguishable from uniformly chosen string $x \epsilon \{0,1\}^n$. Let $G_1$ be the corresponding game:

$$G_1 \begin{cases} s \epsilon S \\ x \epsilon \{0,1\}^n \\ \text{return } [x_k \not= A(x_\bullet)] . \end{cases}$$

For the formal proof, we need to estimate the computational difference of $G_0$ and $G_1$ in terms of security games:

$$Q^B_0 \begin{cases} s \epsilon \{0,1\}^n \\ x \epsilon f(s) \\ \text{return } [B(x) \not= 1] \end{cases} \quad Q^B_1 \begin{cases} x \epsilon \{0,1\}^n \\ \text{return } [B(x) \not= 1] \end{cases}$$

through which the notion of pseudorandomness is defined. Now if we define the adversary as follows:

$$B(x) \begin{cases} \text{return } [x_k \not= A(x_\bullet)] \end{cases}$$

then $Q^B_0 \equiv G^A_0$ and $Q^B_1 \equiv G^A_1$. As $B$ is a valid program and its running time is only by a constant slower than the running time of $A$, games $G_0$ and $G_1$ are $(t, \varepsilon)$-indistinguishable. As the bit $x_k$ is completely independent form $x_\bullet$ in the game $G_1$, we get the desired result:

$$\text{Adv}^\text{hc-pred}_{f,\pi}(A) = |\Pr [G^A_0 = 1] - \frac{1}{2}| = |\Pr [G^A_0 = 1] - \Pr [G^A_1 = 1]| \leq \varepsilon .$$