MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Hard-core predicate based on indistinguishability). *A predicate* π *is a* (t,ε)-unpredictable *also known as* (t,ε)-hardcore predicate *for a function* $f:\mathcal{S}\to\mathcal{X}$ *if for any* t*-time adversary*

$$\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f}(\mathcal{A}) = 2\cdot\left|\Pr\left[s \xleftarrow[u]{} \mathcal{S} : \mathcal{A}(f(s)) = \pi(s)\right] - \tfrac{1}{2}\right| \leq \varepsilon \ .$$

Show that $\pi:\mathcal{S}\to\{0,1\}$ *must be almost regular if* π *is hard-core predicate. Let* $\mathcal{X}_i$ *denote the distribution of* $f(s)$ *for* $s \xleftarrow[u]{} \mathcal{S}_i$ *where* $\mathcal{S}_0 = \{s\in\mathcal{S} : \pi(s) = 0\}$ *and* $\mathcal{S}_1 = \{s\in\mathcal{S} : \pi(s)=1\}$*. Show that if the distributions* $\mathcal{X}_0$ *and* $\mathcal{X}_1$ *are* (t,ε)*-indistinguishable then* π *is also a hardcore predicate. Analyse how the prediction advantage depends on regularity. Is it possible to prove the reverse implication?*

Solution.
Hint: Give alternative definition of hard-core bits in terms of two games $\mathcal{Q}_0$ and $\mathcal{Q}_1$.
Hint: Define $\mathcal{B}$ such that $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_0^{\mathcal{A}}$. What is the corresponding $\mathcal{Q}_1^{\mathcal{B}}$?