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

Exercise (Pseudorandom generator based on hard-core bits of a permutation). *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*

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

Let $\pi : \{0,1\}^n \to \{0,1\}$ be a (t,ε)-hardcore predicate for a permutation $f : \{0,1\}^n \to \{0,1\}^n$. Prove that the concatenation $g_1(s) = f(s)||\pi(s)$ is (t,ε)-pseudorandom generator. Prove that the double-concatenation $g_2(s) = f(f(s))\|\pi(f(s))\|\pi(s)$ is $(t,2\varepsilon)$-pseudorandom generator. Can this proof be generalised for other concatenation functions $g_i(s) = f(\ldots f(f(s))\ldots)\|\pi(f(\ldots f(f(s))\ldots))\|\ldots\pi(f(s))\|\pi(s)$?

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 $\mathcal{Q}_1^{\mathcal{B}}$?