1. Recall that a game is a two-party protocol between the challenger \( G \) and an adversary \( A \) and that the output of the game \( G^A \) is always determined by the challenger. Prove the following claims:

(a) Any hypothesis testing scenario \( H \) can be formalised as a game \( G \) such that \( \Pr[A = b|H] = \Pr[G^A = b] \) for all adversaries \( A \).

(b) For two simple hypotheses \( H_0 \) and \( H_1 \), there is a game \( G \) such that
\[
\text{cd}^t_*(H_0, H_1) = 2 \cdot \max_{A \text{ is } t\text{-time}} |\Pr[G_0^A = 1] - \frac{1}{2}| .
\]

(c) The computational distance between games defined as follows
\[
\text{cd}^t_*(G_0, G_1) = \max_{A \text{ is } t\text{-time}} |\Pr[G_0^A = 1] - \Pr[G_1^A = 1]| .
\]

Show that this quantity is indeed a pseudo-metric:
\[
\text{cd}^t_*(G_0, G_1) = \text{cd}^t_*(G_1, G_0) ,
\]
\[
\text{cd}^t_*(G_0, G_2) \leq \text{cd}^t_*(G_0, G_1) + \text{cd}^t_*(G_1, G_2) .
\]

When is the computational distance a proper metric, i.e.,
\[
\text{cd}^t_*(G_0, G_1) \neq 0 \Leftrightarrow \text{sd}^*_{\text{A}}(G_0, G_1) \neq 0 ?
\]

(?) Usually, the statistical distance \( \text{sd}^*_{\text{A}}(G_0, G_1) \) is defined as a limiting value \( \text{sd}^*_{\text{A}}(G_0, G_1) = \lim_{t \to \infty} \text{cd}^t_*(G_0, G_1) \). Give an alternative interpretation in terms of output distributions.

2. Let \( A \) be a \( t \)-time distinguisher and let \( \alpha(A) = \Pr[A = 1|H_0] \) and \( \beta(A) = \Pr[A = 0|H_1] \) be the ratios of false negatives and false positives. Show that for any \( c \) there exists a \( t + O(1) \)-time adversary \( B \) such that
\[
\alpha(B) = (1 - c) \cdot \alpha(A) \quad \text{and} \quad \beta(B) = c + (1 - c) \cdot \beta(A) .
\]

Are there any practical settings where such trade-offs are economically justified? Give some real world examples.

**Hint:** What happens if you first throw a fair coin and run \( A \) only if you get tail and otherwise output 0?

3. Let \( X_0 \) and \( X_1 \) efficiently sampleable distributions that are \((t, \epsilon)\)-indistinguishable. Show that distributions \( X_0 \) and \( X_1 \) remain computationally indistinguishable even if the adversary can get \( n \) samples.
(a) First estimate computational distances between following games

\[
\begin{array}{l}
G_{00}^A \\
\begin{cases}
  x_0 \leftarrow X_0 \\
x_1 \leftarrow X_0 \\
 \text{return } A(x_0, x_1)
\end{cases}
\end{array}
\quad
\begin{array}{l}
G_{01}^A \\
\begin{cases}
  x_0 \leftarrow X_0 \\
x_1 \leftarrow X_1 \\
 \text{return } A(x_0, x_1)
\end{cases}
\end{array}
\quad
\begin{array}{l}
G_{11}^A \\
\begin{cases}
  x_0 \leftarrow X_1 \\
x_1 \leftarrow X_1 \\
 \text{return } A(x_0, x_1)
\end{cases}
\end{array}
\]

**Hint:** What happens if you feed a sample \( x_0 \leftarrow X_0 \) together an unknown sample \( x_1 \leftarrow X_i \) to \( A \) and use the reply to guess \( i \).

(b) Generalize the argumentation to the case, where the adversary \( A \) gets \( n \) samples from a distribution \( X_i \). That is, define the corresponding sequence of games \( G_{00}^{i_0} \ldots, G_{11}^{i_1} \).

(c) Why do we need to assume that distributions \( X_0 \) and \( X_1 \) are efficiently samplable?

4. Consider the following game, where an adversary \( A \) gets three values \( x_1, x_2 \) and \( x_3 \). Two of them are sampled from the efficiently samplable distribution \( X_0 \) and one of them is sampled from the efficiently samplable distribution \( X_1 \). The adversary wins the game if it correctly determines which sample is taken from \( X_1 \).

(a) Find an upper bound to the success probability if distributions \( X_0 \) and \( X_1 \) are \( (t, \epsilon) \)-indistinguishable.

(b) How does the bound on the success change if we modify the game in the following manner. First, the adversary can first make its initial guess \( i_0 \). Then the challenger reveals \( j \neq i_0 \) such that \( x_j \) was sampled from \( X_0 \) and then the adversary can output its final guess \( i_1 \).

**Hint:** How well the adversary can perform if the challenger gives no samples to the adversary? How can you still simulate the game to the adversary who expects these samples?

5. A predicate \( \pi : \{0, 1\}^n \rightarrow \{0, 1\} \) is said to be an \( \epsilon \)-regular if the output distribution for uniform input distribution is nearly uniform:

\[
|\Pr[s \leftarrow \{0, 1\}^n : \pi(s) = 0] - \Pr[s \leftarrow \{0, 1\}^n : \pi(s) = 1]| \leq \epsilon .
\]

A predicate \( \pi \) is a \( (t, \epsilon) \)-unpredictable also known as \( (t, \epsilon) \)-hardcore predicate for a function \( f : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\ell} \) if for any \( t \)-time adversary

\[
\text{Adv}_{f}^{\text{hc-pred}}(A) = 2 \cdot |\Pr[s \leftarrow \{0, 1\}^n : A(f(s)) = \pi(s)] - \frac{1}{2}| \leq \epsilon .
\]

Prove the following statements.

(a) Any \( (t, \epsilon) \)-hardcore predicate is \( 2\epsilon \)-regular.

(b) For a function \( f : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\ell} \), 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 \( (t, \epsilon) \)-secure pseudorandom generator, then \( \pi_k \) is \( (t, \epsilon) \)-hardcore predicate for \( f_k \).
If a function $f : \{0,1\}^n \rightarrow \{0,1\}^{n+\ell}$ is $(t,\varepsilon_1)$-pseudorandom generator and $\pi : \{0,1\}^n \rightarrow \{0,1\}$ is efficiently computable predicate $(t,\varepsilon_1)$-hardcore, then a concatenation $f_\pi(s) = f(s)||\pi(s)$ is $(t,\varepsilon_1+\varepsilon_2)$-pseudorandom generator.

6. Let $F$ be a $(t,q,\varepsilon)$-pseudorandom function family that maps a domain $M$ to the range $C$. Let $g : M \rightarrow \{0,1\}$ be an arbitrary predicate. What is the success probability of a $t$-time adversary $A$ in the following games?

G\text{A}_0
\begin{align*}
& m \leftarrow M \\
& f \leftarrow F \\
& c \leftarrow f(m) \\
& \text{return } [A(c) = m]
\end{align*}

G\text{A}_1
\begin{align*}
& m \leftarrow M \\
& f \leftarrow F \\
& c \leftarrow f(m) \\
& \text{return } [A(c) = g(m)]
\end{align*}

Establish the same result by using the IND$\Rightarrow$SEM theorem. More precisely, show that the hypothesis testing games

G\text{A}_{m_0}
\begin{align*}
& f \leftarrow F \\
& c \leftarrow f(m_0) \\
& \text{return } A(c)
\end{align*}

G\text{A}_{m_1}
\begin{align*}
& f \leftarrow F \\
& c \leftarrow f(m_1) \\
& \text{return } A(c)
\end{align*}

are $(t,2\varepsilon)$-indistinguishable for all $m_0, m_1 \in M$. 

3