Exercise (Prediction of randomised functions). Let \( g: \mathcal{S} \times \Omega \to \mathcal{Y} \) be a randomised function and let \( f: \mathcal{S} \to \mathcal{X} \) be a function such that any two states \( s_0, s_1 \in \mathcal{S} \) are \((t, \varepsilon)\)-indistinguishable given the output \( f(s_i) \). Prove that a function \( f^*: \mathcal{S} \times \Omega \to \mathcal{X} \) defined as \( f_*(s, \omega) = f(s) \) is also such that any two states \((s_0, \omega_0), (s_1, \omega_1) \in \mathcal{S} \times \Omega \) are \((t, \varepsilon)\)-indistinguishable given the output \( f_*(s_i, \omega_i) \) and that

\[
\text{Adv}_{f,g}^\text{ind}(A) = \text{Adv}_{f_*,g_*}^\text{ind}(A)
\]

where \( g_*(s, \omega) = g(s, \omega) \) is a deterministic function over extended state space \( \mathcal{S} \times \Omega \).

Solution. Indistinguishability of states. For the first part of the proof we must estimate the computational distance of following games:

\[
\mathcal{G}_{s_0, \omega_0}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f(s_0, \omega_0) \\
\text{return } A(x)
\end{align*}
\]

\[
\mathcal{G}_{s_1, \omega_1}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f_*(s_0, \omega_1) \\
\text{return } A(x)
\end{align*}
\]

By the definition of function \( f_* \), we can simplify these games:

\[
\mathcal{G}_{s_0}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f(s_0) \\
\text{return } A(x)
\end{align*}
\]

\[
\mathcal{G}_{s_1, \omega_1}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f_*(s_1, \omega_1) \\
\text{return } A(x)
\end{align*}
\]

Since these games do not depend on \( \omega_0 \) and \( \omega_1 \), we can observe the following games:

\[
\mathcal{G}_{s_0}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f(s_0) \\
\text{return } A(x)
\end{align*}
\]

\[
\mathcal{G}_{s_1}
\]

\[
\begin{align*}
\text{let } x &\leftarrow f_*(s_1) \\
\text{return } A(x)
\end{align*}
\]

By the security assumption for \( f \), the games \( \mathcal{G}_{s_0} \) and \( \mathcal{G}_{s_1} \) is \((t, \varepsilon)\)-indistinguishable. Hence, for any \( t \)-time adversary \( A \), the advantage of distinguishing games \( \mathcal{G}_{s_0, \omega_0} \) and \( \mathcal{G}_{s_1, \omega_1} \) is bounded:

\[
\text{Adv}_{s_0, \omega_0}, (s_1, \omega_1) (A) = \left| \Pr [\mathcal{G}_{s_0, \omega_0}^A = 1] - \Pr [\mathcal{G}_{s_1, \omega_1}^A = 1] \right| \\
= \left| \Pr [\mathcal{G}_{s_0}^A = 1] - \Pr [\mathcal{G}_{s_1}^A = 1] \right| = \text{Adv}_{s_0, \omega_0}, (A) \leq \varepsilon
\]

This proves the desired claim about indistinguishability of extended states.

Guessing advantage. Recall that the advantage \( \text{Adv}_{f,g}^\text{sem}(A) \) can be expressed as the distance between the following games

\[
\mathcal{Q}_0
\]

\[
\begin{align*}
\text{let } x &\leftarrow f(s) \\
\text{return } g(s) \overset{?}{=} A(x)
\end{align*}
\]

\[
\mathcal{Q}_1
\]

\[
\begin{align*}
\text{let } x &\leftarrow f_*(s, \omega) \\
\text{return } g_*(s, \omega) \overset{?}{=} y_0
\end{align*}
\]

where \( y_0 \) is the most probable outcome of \( g(s) \). Analogously, \( \text{Adv}_{f_*,g_*}^\text{sem}(A) \) can be expressed as the distance between the following games

\[
\mathcal{Q}_0
\]

\[
\begin{align*}
\text{let } x &\leftarrow f(s) \\
\text{return } A(x)
\end{align*}
\]

\[
\mathcal{Q}_1
\]

\[
\begin{align*}
\text{let } x &\leftarrow f_*(s, \omega) \\
\text{return } g_*(s, \omega) \overset{?}{=} y_*
\end{align*}
\]
where $y_*$ is the most probable outcome of $g_*(s, \omega)$. First, note that $y_0$ coincides with $y_*$, since by definition

$$y_0 = \arg\max_{y \in Y} \Pr[s \leftarrow S : g(s) \overset{?}{=} y] = \arg\max_{y \in Y} \Pr[s \leftarrow S, \omega \leftarrow \Omega : g(s, \omega) \overset{?}{=} y] = y_* .$$

Second, note that we can explicitly sample the randomness used to evaluate $g$ in the first set of games:

$$\begin{align*}
G_0 & \begin{cases}
    s \leftarrow S \\
    \omega \leftarrow \Omega \\
    x \leftarrow f(s) \\
    \text{return } [g(s, \omega) \overset{?}{=} A(x)]
\end{cases} & \begin{cases}
    s \leftarrow S \\
    \omega \leftarrow \Omega \\
    x \leftarrow f(s) \\
    \text{return } [g(s, \omega) \overset{?}{=} g_*(x) ]
\end{cases}
\end{align*}$$

Now if we substitute the definitions of $f_*$ and $g_*$ into the second set of games, we get games

$$\begin{align*}
Q_0 & \begin{cases}
    s \leftarrow S \\
    \omega \leftarrow \Omega \\
    x \leftarrow f(s) \\
    \text{return } [g(s, \omega) \overset{?}{=} A(x)]
\end{cases} & \begin{cases}
    s \leftarrow S \\
    \omega \leftarrow \Omega \\
    x \leftarrow f(s) \\
    \text{return } [g(s, \omega) \overset{?}{=} y_* ]
\end{cases}
\end{align*}$$

that are identical to the first set of games. Hence,

$$\text{Adv}_{f,g}^{sem}(A) = |\Pr[G_0^A = 1] - \Pr[G_1^A = 1]| = |\Pr[Q_0^A = 1] - \Pr[Q_1^A = 1]| = \text{Adv}_{f,g_*}^{sem}(A)$$

as desired. The claim about prediction success follows.