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

Exercise (Analysis of bad events). *Prove that statistical distance between the games*

```
$\mathcal{G}_0^{\mathcal{A}}$
    $y_0 \leftarrow \perp$
    For $i \in \{1,\ldots,q\}$ do
        $x_i \leftarrow \mathcal{A}(y_{i-1})$
        if $x_i = \perp$ then break
        $y_i \xleftarrow{u} \mathcal{M}$
        if $y_i \in \{y_1,\ldots,y_{i-1}\}$ then
            do nothing
    return $\mathcal{A}$

$\mathcal{G}_1^{\mathcal{A}}$
    $y_0 \leftarrow \perp$
    For $i \in \{1,\ldots,q\}$ do
        $x_i \leftarrow \mathcal{A}(y_{i-1})$
        if $x_i = \perp$ then break
        $y_i \xleftarrow{u} \mathcal{M}$
        if $y_i \in \{y_1,\ldots,y_{i-1}\}$ then
            $y_i \xleftarrow{u} \mathcal{M} \setminus \{y_1,\ldots,y_{i-1}\}$
    return $\mathcal{A}$
```

is the cumulative probability that one of the if branches gets executed.

Solution. Let us first consider the simplified case where the adversary $\mathcal{A}$ makes exactly two queries. Then the corresponding games can be simplified:

```
$\mathcal{G}_0^{\mathcal{A}}$
    $x_1 \leftarrow \mathcal{A}$
    $y_1 \xleftarrow{u} \mathcal{M}$
    $x_2 \leftarrow \mathcal{A}(y_1)$
    $y_2 \xleftarrow{u} \mathcal{M}$
    if $y_2 = y_1$ then
        do nothing
    return $\mathcal{A}(y_2)$

$\mathcal{G}_1^{\mathcal{A}}$
    $x_1 \leftarrow \mathcal{A}$
    $y_1 \xleftarrow{u} \mathcal{M}$
    $x_2 \leftarrow \mathcal{A}(y_1)$
    $y_2 \xleftarrow{u} \mathcal{M}$
    if $y_2 = y_1$ then
        $y_2 \xleftarrow{u} \mathcal{M} \setminus \{y_1\}$
    return $\mathcal{A}(y_2)$
```

We present two ways how to analyse this problem. First, we can do direct computations of probabilities and derive

$$\begin{aligned}
\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] &= \Pr\left[y_1 = y_2 \wedge \mathcal{A}(y_2) = 1\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right]\\
&\leq \Pr\left[y_1 = y_2\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right] \quad ,\\
\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] &= \Pr\left[y_1 = y_2 \wedge \mathcal{A}(y_2) = 1\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right]\\
&\geq \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right] \quad ,\\
\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] &= \Pr\left[y_1 = y_2 \wedge \mathcal{A}(y_2) = 1\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right]\\
&\geq \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right] \quad ,\\
\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] &= \Pr\left[y_1 = y_2 \wedge \mathcal{A}(y_2) = 1\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right]\\
&\leq \Pr\left[y_1 = y_2\right] + \Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right] \quad .
\end{aligned}$$

Note that probabilities $\Pr\left[y_1 = y_2\right]$ and $\Pr\left[y_1 \neq y_2 \wedge \mathcal{A}(y_2) = 1\right]$ are exactly the same in both games (a formal proof is lengthy but straightforward) and thus combining all these inequalities yields

$$-\Pr\left[y_1 = y_2\right] \leq \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \leq \Pr\left[y_1 = y_2\right] \quad .$$

As a second possible solution let us align use of randomness in both games. To make it absolutely clear, let us consider the following games:

```
$\mathcal{G}_0^{\mathcal{A}}$
    $x_1 \leftarrow \mathcal{A}$
    $y_1 \xleftarrow[u]{} \mathcal{M}$
    $x_2 \leftarrow \mathcal{A}(y_1)$
    $y_2 \xleftarrow[u]{} \mathcal{M}$
    if $y_2 = y_1$ then
        $z \xleftarrow[u]{} \mathcal{M} \setminus \{y_1\}$
    return $\mathcal{A}(y_2)$
```

```
$\mathcal{G}_1^{\mathcal{A}}$
    $x_1 \leftarrow \mathcal{A}$
    $y_1 \xleftarrow[u]{} \mathcal{M}$
    $x_2 \leftarrow \mathcal{A}(y_1)$
    $y_2 \xleftarrow[u]{} \mathcal{M}$
    if $y_2 = y_1$ then
        $y_2 \xleftarrow[u]{} \mathcal{M} \setminus \{y_1\}$
    return $\mathcal{A}(y_2)$
```

As both games now use the same set of randomness $\omega \in \Omega_{\mathcal{A}} \times \mathcal{M} \times \mathcal{M} \setminus \{y_1\}$ where $\Omega_{\mathcal{A}}$ stands for the randomness space of $\mathcal{A}$, we can treat both games as deterministic functions $\mathcal{G}_0^{\mathcal{A}}(\omega)$ and $\mathcal{G}_1^{\mathcal{A}}(\omega)$. By the construction $\mathcal{G}_0^{\mathcal{A}}(\omega) \neq \mathcal{G}_1^{\mathcal{A}}(\omega)$ only if we reach the if branch. Consequently,

$$\left\{\omega : \mathcal{G}_0^{\mathcal{A}}(\omega) \neq \mathcal{G}_1^{\mathcal{A}}(\omega)\right\} \subseteq \{\omega : y_1(\omega) \neq y_2(\omega)\}$$

and thus also by definition

$$\Pr\left[\omega : \mathcal{G}_0^{\mathcal{A}}(\omega) \neq \mathcal{G}_1^{\mathcal{A}}(\omega)\right] \leq \Pr\left[\omega : y_1(\omega) \neq y_2(\omega)\right] .$$

Now note that

$$\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \leq \Pr\left[\omega : \mathcal{G}_0^{\mathcal{A}}(\omega) \neq \mathcal{G}_1^{\mathcal{A}}(\omega)\right] \quad ,$$

since all other terms cancel out. The claim follows.

To give a general proof, lets modify the code so that the used randomness is again aligned:

```
$\mathcal{G}_0^{\mathcal{A}}$
    $y_0 \leftarrow \perp$
    For $i \in \{1, \ldots, q\}$ do
        $x_i \leftarrow \mathcal{A}(y_{i-1})$
        if $x_i = \perp$ then break
        $y_i \xleftarrow[u]{} \mathcal{M}$
        if $y_i \in \{y_1, \ldots, y_{i-1}\}$ then
            $z \xleftarrow[u]{} \mathcal{M} \setminus \{y_1, \ldots, y_{i-1}\}$
    return $\mathcal{A}$
```

```
$\mathcal{G}_1^{\mathcal{A}}$
    $y_0 \leftarrow \perp$
    For $i \in \{1, \ldots, q\}$ do
        $x_i \leftarrow \mathcal{A}(y_{i-1})$
        if $x_i = \perp$ then break
        $y_i \xleftarrow[u]{} \mathcal{M}$
        if $y_i \in \{y_1, \ldots, y_{i-1}\}$ then
            $y_i \xleftarrow[u]{} \mathcal{M} \setminus \{y_1, \ldots, y_{i-1}\}$
    return $\mathcal{A}$
```

Again by construction, the deterministic functions $\mathcal{G}_0^{\mathcal{A}}(\omega)$ and $\mathcal{G}_1^{\mathcal{A}}(\omega)$ can diverge $\mathcal{G}_0^{\mathcal{A}}(\omega) \neq \mathcal{G}_1^{\mathcal{A}}(\omega)$ on arguments ω for which some if branch is executed. Hence

$$\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \leq \Pr\left[\omega : \text{some if branch is reached}\right] \quad .$$

Remark. This divergence argument generalises for any game pair with aligned randomness. As if branches containing different code can be aligned to use the same randomness, the statistical distance of games with different if branches is always bounded by the probability of executing one of these branches. The corresponding code transformation is known as the Bad reduction schema.