TD n° 1

Hugo SALOU
ENS M1

Exercise 1. Statistical distance.

Q1. Suppose $\Delta(X, Y) = 0$. Let $\mathcal{A}$ be some adversary.

Then

$$\mathrm{Adv}_{\mathcal{A}}(X,Y) = \left| P_r[\mathcal{A}(X) = 1] - P_r[\mathcal{A}(Y) = 1] \right|$$

$$\leq 2 \times \Delta(\mathcal{A}(X), \mathcal{A}(Y)) \underset{(Q2a)}{\leq} 2 \times \Delta(X,Y) = 0.$$

Q2a.

$$\Delta(f(X), f(Y)) = \frac{1}{2} \sum_{a \in S} \left| P_r[f(X) = a] - P_r[f(Y) = a] \right|$$

$$= \frac{1}{2} \sum_{b \in f^{-1}(S)} \left| P_r[X = b] - P_r[Y = b] \right|$$

$$\leq \frac{1}{2} \sum_{b \in A} \left| P_r[X = b] - P_r[Y = b] \right| = \Delta(X,Y).$$

Q2b.

$$\Delta((X,Z),(Y,Z)) = \frac{1}{2} \sum_{(a,z) \in A \times \mathcal{Z}} \left| P_r[(X,Z) = (a,z)] - P_r[(Y,Z) = (a,z)] \right|$$

(by independance)

$$= \frac{1}{2} \sum_{a \in A} \sum_{z \in \mathcal{Z}} P_r[Z = z] \left| P_r[X = a] - P_r[Y = a] \right|$$

$$= \frac{1}{2} \sum_{a \in A} \underbrace{1} \left| P_r[X = a] - P_r[Y = a] \right| = \Delta(X,Y).$$

Q2c. (Should we define f' and R ?)

$$\Delta(f(X), f(Y)) = \frac{1}{2} \sum_{a \in S} \left| P_r[f(X) = a] - P_r[f(Y) = a] \right|$$

$$= \frac{1}{2} \sum_{a \in S} \left| P_r[f'(X,R) = a] - P_r[f(X,R) = a] \right|$$

$$= \Delta(f'(X,R), f'(Y,R)).$$

Then, as f' is deterministic, we have

$$\Delta(f'(X,R), f(Y,R)) \leq \Delta((X,R),(Y,R)) = \Delta(X,Y).$$

Q3.

$$\begin{aligned} \mathrm{Adv}_{\mathcal{A}}(X,Y) &\leq \Delta(\mathcal{A}(X), \mathcal{A}(Y)) \\ &\leq \Delta(X,Y) \end{aligned}$$

Q4.

$$\Delta(G(U(\{0,1\}^{\ell})), U(\{0,1\}^{n}))$$

Exercise 2. About the advantage definition.

Q1. c.f. notes

Q2.
$$\begin{aligned} \mathrm{Adv}_2(\mathcal{A}) &= \left| \Pr[\mathcal{A} \xrightarrow{\mathrm{Exp}_0} 0] + \Pr[\mathcal{A} \xrightarrow{\mathrm{Exp}_1} 1] - 1 \right| \\ &= \left| \Pr[\mathcal{A} \xrightarrow{\mathrm{Exp}_0} 1] - \Pr[\mathcal{A} \xrightarrow{\mathrm{Exp}_1} 1] \right| \\ &= \mathrm{Adv}_1(\mathcal{A}) \end{aligned}$$

Exercise 3. A weird distinguisher...

Q1. Do N samples from D_0 and N from D_1, we will write them $a_1, \dots, a_N$ and $b_1, \dots, b_N$.

We define $\mu_i := \Pr[\mathcal{A} \xrightarrow{\mathrm{Exp}^i} 1]$. We have that:

$$\Pr[|\bar{B} - \mu_1| \geq \varepsilon) \leq 2\exp(-2N\varepsilon^2)$$

$\forall \varepsilon > 0$,

where $\bar{B} = \sum_{j=1}^{N} b_j$ and similarly for $\bar{A}$. Thus,

$$\Pr[\mathrm{Adv}_{\mathcal{A}} \leq 2\varepsilon + |\bar{B} - \bar{A}|] \geq 1 - 4\exp(-2N\varepsilon^2).$$

so, $$\Pr[|\mathrm{Adv}_{\mathcal{A}} - |\bar{B} - \bar{A}|| \leq 2\varepsilon] \geq 1 - 4\exp(-2N\varepsilon^2).$$

Q2. Define $\mu_b := \Pr[\mathcal{A} \xrightarrow{Expt_b} 1]$.

$$\begin{aligned} Adv_p(\mathcal{A}') &= \mu_0(1-\mu_0)(\mu_1-\mu_0) + \mu_0(1-\mu_1)(\mu_0-\mu_1) \\ &= (\mu_1-\mu_0)(\mu_1 - \mu_0\mu_1 - \mu_0 + \mu_0\mu_1) \\ &= \varepsilon^2 \end{aligned}$$