Assignment #9

Hugo SALOU

1) We will write $P(x)$ (resp. $Q(x)$) for $\Pr_{X\sim P}[X=x]$ (resp. $\Pr_{X\sim Q}[X=x]$).

Here is the algorithm distinguishing P and Q:

```
for an input $x \in R$,
• if $P(x) > Q(x)$ then output "P!"
• otherwise output "Q!".
```

We have the following lemma:

$$\max(a,b) = \frac{a+b}{2} + \frac{|a-b|}{2} \qquad \text{when } a,b \geq 0$$

(if $a \geq b$, then $\frac{a+b}{2} + \frac{a-b}{2} = a$ and symmetrically for $b \geq a$).

$$\Pr[\text{success}] = \frac{1}{2} \cdot \Pr_{x\sim P}[P(x) > Q(x)] + \frac{1}{2}\Pr_{x\sim Q}[P(x) \leq Q(x)]$$

$$= \frac{1}{2}\sum_{\substack{x\in R \\ P(x)>Q(x)}} P(x) + \frac{1}{2}\sum_{\substack{x\in R \\ P(x)\leq Q(x)}} Q(x)$$

$$= \frac{1}{2}\sum_{x\in R} \max(P(x), Q(x))$$

$$= \underbrace{\frac{1}{2}\sum_{x\in R} \frac{P(x)+Q(x)}{2}}_{\sum_{x\in R} P(x) = \sum_{x\in R} Q(x) = 1} + \underbrace{\frac{1}{2}\sum_{x\in R}\frac{|P(x)-Q(x)|}{2}}_{\frac{1}{2}\Delta(P,Q)}$$

$$= \frac{1}{2} + \frac{1}{2}\Delta(P,Q)$$

So, this algorithm distinguishes between P and Q with a success probability of $\frac{1}{2}+\frac{1}{2}\Delta(P,Q)$.

2) Let $p(x)$ be the probability that a distinguisher $\mathcal{A}$ between P and Q outputs "P!" on the input $x \in R$.

$$\Pr[\text{success}] = \frac{1}{2}\Pr_{x\sim P}[\mathcal{A}\rightsquigarrow\text{"P!"}] + \frac{1}{2}\Pr_{x\sim Q}[\mathcal{A}\rightsquigarrow\text{"Q!"}]$$

$$= \frac{1}{2}\sum_{x\in R} p(x)\,P(x) + \frac{1}{2}\sum_{x\in R}(1-p(x))\,Q(x)$$

$$= \frac{1}{2}\sum_{x\in R}\big(Q(x) + p(x)\big(P(x)-Q(x)\big)$$

$$= \frac{1}{2} + \frac{1}{2}\sum_{x\in R} p(x)\big(P(x)-Q(x)\big)$$

$$\leq \frac{1}{2} + \frac{1}{2}\sum_{x\in R}\max\big(0,\ P(x)-Q(x)\big)$$

as $p(x)\in[0,1]$.

And, we have that

$$0 = \sum_{x\in R} P(x) - \sum_{x\in R} Q(x) = \sum_{x\in R}\big(P(x)-Q(x)\big) = \sum_{P(x)>Q(x)}\big(P(x)-Q(x)\big) + \sum_{P(x)<Q(x)}\big(P(x)-Q(x)\big)$$

then

$$\sum_{P(x)>Q(x)}|P(x)-Q(x)| = -\sum_{P(x)<Q(x)}\big(P(x)-Q(x)\big) = \sum_{P(x)<Q(x)}\big(Q(x)-P(x)\big)$$

$$= \sum_{P(x)<Q(x)}|P(x)-Q(x)|$$

thus

$$\sum_{r\in R} |P(r) - Q(r)| = \sum_{P(r) > Q(r)} |P(r) - Q(r)| + \sum_{P(r) < Q(r)} |P(r) - Q(r)|$$

$$= 2 \cdot \sum_{P(r) > Q(r)} (P(r) - Q(r))$$

$$= 2 \cdot \sum_{r\in R} \max(0, P(r) - Q(r))$$

and we can conclude that

$$\Pr[\text{success}] \leq \frac{1}{2} + \frac{1}{2} \sum_{r\in R} \max(0, P(r) - Q(r))$$

$$\leq \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \sum_{r\in R} |P(r) - Q(r)|$$

$$\leq \frac{1}{2} + \frac{1}{2} \Delta(P, Q)$$

and so the success probability of the algorithm from 1) is optimal.

End of Assignment # 9