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

Exercise (Convex closure for distinguishers). *Let $\mathcal{A}$ and $\mathcal{B}$ be a t-time distinguishers with the following ratios for false negatives and false positives:*

$$\alpha(\mathcal{A}) = \Pr[\mathcal{A}(x) = 0|\mathcal{H}_1] \qquad \beta(\mathcal{A}) = \Pr[\mathcal{A}(x) = 1|\mathcal{H}_0]$$
$$\alpha(\mathcal{B}) = \Pr[\mathcal{B}(x) = 0|\mathcal{H}_1] \qquad \beta(\mathcal{B}) = \Pr[\mathcal{B}(x) = 1|\mathcal{H}_0]$$

Show that for any $\lambda \in [0, 1]$ there exists a $t + O(1)$-time adversary $\mathcal{C}$ such that

$$\alpha(\mathcal{C}) = \lambda \cdot \alpha(\mathcal{A}) + (1 - \lambda) \cdot \alpha(\mathcal{B}) \ ,$$
$$\beta(\mathcal{C}) = \lambda \cdot \beta(\mathcal{A}) + (1 - \lambda) \cdot \beta(\mathcal{B}) \ .$$

Explain the consequences of this result by sketching the region of achievable tradeoffs on the false negative $\alpha(\cdot)$ and false positive $\beta(\cdot)$ plane for many tradeoffs.

Solution. Let us first construct the required distinguisher $\mathcal{C}$. The construction is as follows:

$\mathcal{C}_\lambda(x)$
$\lambda_* \xleftarrow{u} [0, 1]$
if $\lambda_* \leq \lambda$ then **return** $\mathcal{A}(x)$
return $\mathcal{B}(x)$.

As we first sample λ_* uniformly from the range $[0, 1]$, the distinguisher returns the output of $\mathcal{A}$ on the given input x with probability exactly λ. Otherwise, the output of $\mathcal{B}(x)$ is returned instead, with probability $1 - \lambda$. Let us ratios for false positives and false negatives for $\mathcal{C}$. For false negatives, we get

$$\begin{aligned}
\alpha(\mathcal{C}) &= \Pr[\mathcal{C}(x) = 0|\mathcal{H}_1] \\
&= \Pr[\lambda_* \leq \lambda] \cdot \Pr[\mathcal{A}(x) = 0|\mathcal{H}_1] + \Pr[\lambda_* > \lambda] \cdot \Pr[\mathcal{B}(x) = 0|\mathcal{H}_1] \\
&= \lambda \cdot \Pr[\mathcal{A}(x) = 0|\mathcal{H}_1] + (1 - \lambda) \cdot \Pr[\mathcal{B}(x) = 0|\mathcal{H}_1] \\
&= \lambda \cdot \alpha(\mathcal{A}) + (1 - \lambda) \cdot \alpha(\mathcal{B})
\end{aligned}$$

which is exactly the required ratio. Similarly, for false positives:

$$\begin{aligned}
\beta(\mathcal{C}) &= \Pr[\mathcal{C}(x) = 1|\mathcal{H}_0] \\
&= \Pr[\lambda_* \leq \lambda] \cdot \Pr[\mathcal{A}(x) = 1|\mathcal{H}_0] + \Pr[\lambda_* > \lambda] \cdot \Pr[\mathcal{B}(x) = 1|\mathcal{H}_0] \\
&= \lambda \cdot \Pr[\mathcal{A}(x) = 1|\mathcal{H}_0] + (1 - \lambda) \cdot \Pr[\mathcal{B}(x) = 1|\mathcal{H}_0] \\
&= \lambda \cdot \beta(\mathcal{A}) + (1 - \lambda) \cdot \beta(\mathcal{B})
\end{aligned}$$

Thus, this construction achieves the required ratios for false positives and negatives for any $\lambda \in [0, 1]$.

Let us now analyse the running time of $\mathcal{C}$. The distinguisher needs to sample a random value from $[0, 1]$, do one comparison and then call either $\mathcal{A}$ or $\mathcal{B}$. For obvious reason, it is not possible to sample real numbers with ordinary computers. Hence, this step is actually approximated by sampling n random coin-flips and consequently we achieve only tradeoff points $\lambda \in \{0, 2^{-n}, 2 \cdot 2^{-n}, \ldots, 2^n \cdot 2^{-n}\}$. As a result, the running time of $\mathcal{C}$ is clearly $t + O(n)$ whenever the running times of $\mathcal{A}$ and $\mathcal{B}$ are below t. Note that the precision grows exponentially with the parameter n and thus achieving desired precision is not a practical problem.

Intuitively, this result shows that it is always possible to combine distinguishers $\mathcal{A}$ and $\mathcal{B}$ such that the resulting distinguisher $\mathcal{C}$ has averaged false positive and false negative ratios. If the ratios of false negatives and false positives differ, then it is possible to seek different balance points between. Figure 1 visualises basic properties of such tradeoffs. Each distinguisher can be viewed as a point in the false negative false positive plane. Achievable tradeoffs are on the line between $\mathcal{A}$ and $\mathcal{B}$. Black segments on the axis show achievable trade-off regions for false negatives and for false positives, respectively. Dash-dotted diagonal lines show equilines for aggregate error γ. For obvious reasons the aggregate error of the tradeoff is always larger than

the aggregate error of the better distinguisher. In other words, the increase in false positives is always larger than the decrease in false negatives and vice versa. The only exception to this rule is the setting where both distinguishers have the same aggregate error. In this case, the tradeoff is the zero sum game.

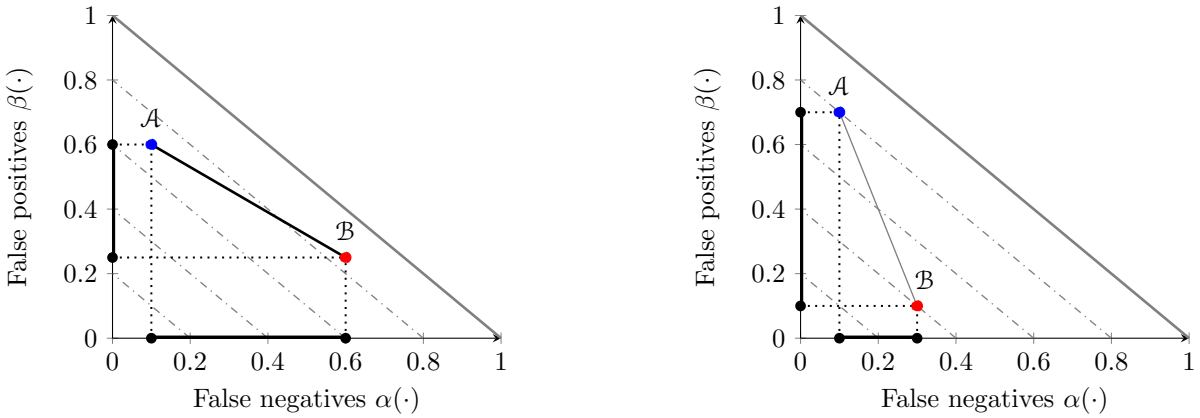

Figure 1: Nature of tradeoff between two distinguishers $\mathcal{A}$ and $\mathcal{B}$

Same principles apply if there are many distinguishers to choose from. However, not all of them are useful, as tradeoffs between different distinguishers might have better parameters. Figure 2 describes a distinguishing profile where some classifiers are useless. As there are trivial distinguishers with parameters $(0, 1)$ and $(1, 0)$ and distinguishers with aggregate error $\gamma > 1$ can be inverted to improve aggregate error, the distinguishing profile is a convex-cup line below the line $\alpha + \beta = 1$. Since the lower bound on aggregate error is determined by statistical distance, the distinguishing profile must be above $\alpha + \beta = 1 - \mathsf{sd}(\mathcal{X}_0, \mathcal{X}_1)$. For the same reason the closest point to the corner on the profile determines the computational distance $\mathsf{cd}^t_x(\mathcal{X}_0, \mathcal{X}_1)$.

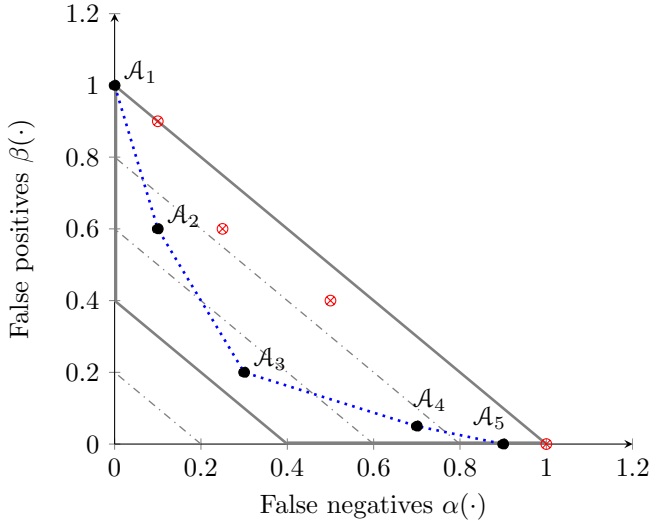

Figure 2: Distinguishing profile is nearly convex-cup line as all distinguishes worse than the averages of distinguisher pairs should be discarded. Discrepancies form convex-cup line are caused by running time constraints. The higher the the bound on the running time is the closer to the corner the profile moves. At limit it is completely determined by the likelihood ratio test.