Cryptography for Computer Scientists 2018/19 Oct 3, 2018

Exercises 1

Stefan Dziembowski MIM UW

Let A and B be two random variables that take values from some set finite $\mathcal{X}$. Define the *statistical distance between A and B* as

$$\Delta(A\,;B) := \tfrac{1}{2} \cdot \sum_{x \in \mathcal{X}} \left| \Pr[A = x] = \Pr[B = x] \right|,$$

and *statistical distance of A from uniformity* as

$$d(A) := \Delta(A\,;U),$$

where U has uniform distribution over $\mathcal{X}$. Analogously Δ can be defined as a distance between two *probability distributions* $\alpha, \beta : \mathcal{X} \to [0,1]$ as

$$\Delta(\alpha\,;\beta) := \Delta(A\,;B),$$

where A and B are random variables (taking values from $\mathcal{X}$) that are distributed according to α and β (respectively). A similar convention applies to the distance d from uniformity.

Exercise 1: An alternative definition of statistical distance

Show that for every A and B we have

$$\Delta(A, B) = \sum_{x : \Pr[A = x] > \Pr[B = x]} \Pr[A = x] - \Pr[B = x]\,.$$

Exercise 2: An interpretation of statistical distance

Let α_0 and α_1 be two distributions over some set $\mathcal{X}$. Consider the following game played by a computationally unbounded machine $\mathcal{M}$ (that knows α_0 and α_1):

1. A uniformly random bit $B \leftarrow \{0, 1\}$ is chosen.
2. A value x is sampled according to distribution α_B and sent to $\mathcal{M}$.
3. $\mathcal{M}$ receives x and produces output B'.

We say that $\mathcal{M}$ *won the game* if $B = B'$. Show that

$$\forall_{\mathcal{M}} \Pr[\mathcal{M} \text{ wins the game}] \leq \frac{1 + \Delta(\alpha_0\,;\alpha_1)}{2}. \tag{1}$$

For every α_0 and α_1 show $\mathcal{M}$ that in achieves equality in (1).

Exercise 3: Permuting does not change the distance

Show that for every two random variable A and B that take values from some set finite set $\mathcal{X}$, and every bijection $f : \mathcal{X} \to \mathcal{X}$ we have that

$$\Delta(f(A)\,;f(B)) = \Delta(A\,;B).$$

Deduce from this that $d(f(A)) = d(A)$.

Exercise 4: Statistical distance as a metric

Let Π be a set of all probability distributions over some finite set $\mathcal{X}$. Prove that Δ is a *metric* on this set, i.e., it satisfies the following axioms:

- *non-negativity:* for every $\alpha, \beta \in \Pi$ we have $\Delta(\alpha\,;\beta) \geq 0$,
- *identity of indiscernibles:* for every $\alpha, \beta \in \Pi$ we have that $\Delta(\alpha\,;\beta) = 0$ implies that $\alpha = \beta$,
- *symmetry:* for every $\alpha, \beta \in \Pi$ we have that $\Delta(\alpha\,;\beta) = \Delta(\beta\,;\alpha)$, and
- *triangle inequality:* for every $\alpha, \beta, \gamma \in \Pi$ we have that $\Delta(\alpha\,;\gamma) \leq \Delta(\alpha\,;\beta) + \Delta(\beta\,;\gamma)$.

Exercise 5: One-time pad with imperfect randomness

Let $(\mathsf{Enc}, \mathsf{Dec})$ be the one-time pad encryption scheme for messages from set $\{0,1\}^t$. Suppose a key K is chosen from $\{0,1\}^t$ according to some distribution α. Consider the guessing game as from the definition of semantic security, that is played between a machine $\mathcal{A}$ and an oracle Ω (however, this time assume that $\mathcal{A}$ is computationally unbouded):

1. $\mathcal{A}$ produces two messages $m_0, m_1 \in \{0,1\}^t$ and sends them to Ω.
2. Ω selects $B \leftarrow \{0,1\}$ uniformly at random, samples K according to α and computes $c = \mathsf{Enc}(K, m_B)$, and sends c to $\mathcal{A}$.
3. $\mathcal{A}$ receives c and produces as output B'

(we assume $\mathcal{A}$ knows α). We say that $\mathcal{M}$ *won the game* if $B = B'$. Show that

$$\forall_{\mathcal{A}} \Pr[\mathcal{A} \text{ wins the game}] \leq \tfrac{1}{2} + d(\alpha).$$

Exercise 6: Conditional statistical distance

Let A be a random variable over some set $\mathcal{X}$ and let B be a random variable over a set $\mathcal{Y}$. Define the *statistical distance of A from uniformity conditioned on B* as

$$d(A|B) := \sum_{b \in \mathcal{Y}} \mathbb{P}\,(B = b) \cdot d(P_{A|B=b}).$$

Show that $d(A|B) = \Delta((A,B)\,;(U_{\mathcal{X}}, B))$, where $U_{\mathcal{X}}$ is a random variable with uniform distribution over $\mathcal{X}$ and independent from B.
Can you find a game-based interpretation of $d(A|B)$ similar to the one in Ex. 2?

Exercise 7: Noticeable functions

A function μ is noticeable iff there exists $c \in \mathbb{N}$ and $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$ we have that $|\mu(n)| \geq n^{-c}$. Answer the following questions:

(a) Is every noticeable function non-negligible?

(b) Is every non-negligible function noticeable?