

Homework

Cryptography course PhD Open

Stefan Dziembowski

Let α, α' be probability distributions over some set \mathcal{A} . Recall that the *statistical distance* $\delta(\alpha; \alpha')$ between α and α' is defined as

$$\delta(\alpha; \alpha') := \frac{1}{2} \sum_{a \in \mathcal{A}} |\alpha(a) - \alpha'(a)|.$$

Let $\xi_{\mathcal{A}}$ denote a uniform distribution over \mathcal{A} . Then $d(\alpha)$ denotes the distance of α from uniform, i.e.:

$$d(\alpha) := \delta(\alpha, \xi_{\mathcal{A}}).$$

We can extend these notions to random variables: for two random variables A and A' by writing $\delta(A; A')$ and $d(A)$ we will mean $\delta(P_A, P_{A'})$ and $d(P_A)$ (resp.). If E is a random event then $\delta(A; A'|E)$ and $d(A|E)$ denotes $\delta(P_{A|E}, P_{A'|E})$ and $d(P_{A|E})$ (resp.).

For a random variable B (distributed over \mathcal{B}) let $d(A|B)$ denote the *distance of A from uniform, conditioned on B* , defined as the following expected value:

$$E(f(B)),$$

where $f(b) := d(A|B = b)$. In other words $d(A|B)$ denotes the expected distance of A from uniform, assuming one knows the value of B .

Exercise 1 Let A, B be random variables. Suppose A is distributed over some set \mathcal{A} , and let $U_{\mathcal{A}}$ be a random variable distributed uniformly over \mathcal{A} (suppose $U_{\mathcal{A}}$ is independent on A, B). Show that¹

$$d(A|B) = \delta((A, B); (U, B)).$$

¹Notation: if $\{A_i : \Omega \rightarrow \mathcal{A}_i\}_{i=1}^n$ are random variables then by (A_1, \dots, A_n) we mean a random variable \vec{A} defined for every $w \in \Omega$ as

$$\vec{A}(w) = (A_1(w), \dots, A_n(w)).$$

Exercise 2 Let A_1, \dots, A_n be random variables. Show that

$$d((A_1, \dots, A_n)) \leq \sum_{i=1}^n d(A_i | (A_1, \dots, A_{i-1})).$$

Exercise 3 Let K, R and U be independent random variables, such that K and U are distributed over the same set, and U is uniform. Let f be some function. Show that

$$d(f(K, R) | K) \leq d(f(U, R) | U) + d(K).$$

Exercise 4 Let $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be a function such that for every S we have $|G(S)| = 2t \cdot |S|$ (for some constant t). Consider the following game between the adversary \mathcal{A} and an oracle Ω .

1. The oracle Ω takes as input parameters m , selects a random string $S \in \{0, 1\}^m$ and sets $x = (x_1, \dots, x_{2mt}) := G(S)$. The oracle sends 1^m to the adversary \mathcal{A} .
2. The adversary chooses $i \in \{1, \dots, 2m\}$ and sends it to the oracle.
3. The oracle sends $(x_1, \dots, x_{t(i-1)})$ to the adversary.
4. The oracle selects a random bit $b \in \{0, 1\}$ and:
 - (a) if $b = 0$ the oracle sends $(x_{t(i-1)+1}, \dots, x_{ti})$ to the adversary,
 - (b) if $b = 1$ the oracle sends a random string of t bits to the adversary.
5. The adversary outputs $b' \in \{0, 1\}$. We say that he won the game if $b = b'$.

Suppose that every polynomial time adversary guesses b with probability at most $0.5 + \mu(m)$ (where μ negligible). Show that this implies that G is a cryptographic pseudorandom generator. How to interpret this result for $t = 1$?

Think about the similarities between Exercises 2 and 4.