Problem Sheet 2

1. (i) Prove that the statistical distance $\delta(P_1, P_2)$ of two distributions P_1 and P_2 on a finite set Ω is equal to

$$\delta(P_1, P_2) = \frac{1}{2} \sum_{\omega \in \Omega} |P_1(\omega) - P_2(\omega)|,$$

that is,

$$\delta(P_1, P_2) = \frac{1}{2} ||P_1 - P_2||_1$$

viewing P_1 and P_2 as vectors (i.e., elements) in $\mathbb{R}^\Omega$.

(ii) To which norm is related the concept of ε-robustness?

2. Show that for every mapping $f : \{0,1\}^n \to \{0,1\}^m$ with $m > n$, there exists an $(n, n-1)$-source P such that

$$\delta(\mathcal{P}_{f,P}, \mathbb{U}_m) \geq \frac{1}{2}.$$

3. (i) Use the fact that for a Boolean function $f : \{0,1\}^n \to \{0,1\}$, we have

$$f(x_1, \ldots, x_n) = (x_n \wedge f(x_1, \ldots, x_{n-1}, 1)) \vee (\neg x_n \wedge f(x_1, \ldots, x_{n-1}, 0))$$

to prove that f can be computed by a circuit of size at most $2^{n+2} - 4$.

(ii) Show that there exists a circuit C of size $O(1)$ such that

$$\mathbb{P}_{x \sim \mathrm{U}_n}[C(x) = f(x)] \geq \frac{1}{2}.$$

4. We consider two distributions P_1 on $\{0,1\}^{n_1}$ and P_2 on $\{0,1\}^{n_2}$, and a map

$$T : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}.$$

Assume that

$$\mathbb{P}_{(x,y) \sim P_1 \times P_2}[T(x,y) = 1] > \frac{1}{2} + \delta$$

for some $\delta > 0$. Show that there exists $y_0 \in \{0,1\}^{n_2}$ such that

$$\mathbb{P}_{x \sim P_1}[T(x, y_0) = 1] > \frac{1}{2} + \delta.$$

Bitte wenden!

5. The *minimal entropy* of a probability distribution P on a finite set Ω is defined as

$$H_\infty(P) := \min_{\omega \in \Omega, P(\omega) > 0} -\log P(\omega).$$

Given any two probability distributions P_1 and P_2 on $\{0,1\}^n$, we define $P := P_1 + P_2$ as the convolution of P_1 and P_2, i.e.,

$$P(\omega) = \sum_{\omega_1 \in \{0,1\}^n} P_1(\omega_1) P_2(\omega - \omega_1),$$

where in the identity above, we view $\{0,1\}^n$ as a vector space over $\mathbb{Z}/2\mathbb{Z}$.

(i) Prove that a distribution P is a (n,k)-source if and only if $H_\infty(P) \geq k$.

(ii) Let P_1 and P_2 be two probability distribution on $\{0,1\}^n$. Prove that

$$H_\infty(P_1 + P_2) \geq \max\{H_\infty(P_1), H_\infty(P_2)\}.$$