D-MATH Topics in Mathematics of Computer Science HS 2013
Dr. M. Cochand

Problem Sheet 1

1. A subset $X \subseteq \mathbb{R}^n$ is *convex* if for every two points $x, y \in X$ and for every real $0 \leq \lambda \leq 1$, the point $\lambda x + (1-\lambda)y$ belongs to X. A *convex combination* of a finite set of points $x_1, x_2, \ldots, x_k \in X$ is any point of the form $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_k x_k$, where $\lambda_i \geq 0$ for $i = 1, 2, \ldots, k$ and $\sum_{i=1}^{k} \lambda_i = 1$.

(i) For each set $A \subseteq \mathbb{R}^n$, let CH(A) denote the set of all convex combinations of finite subsets of A. Prove that $A \subseteq$ CH(A) and CH(A) is convex.

(ii) Show that CH(A) is the *smallest* convex set that contains A, i.e., if B is any convex set containing A, then CH$(A) \subseteq B$.

(iii) Show that for fixed n and k, the set C of (n, k)-sources is convex.

(iv) An *extreme point* of a convex set X is a point $x \in X$ such that if $x = \lambda y + (1 - \lambda)z$, with $y, z \in X$ and $0 \leq \lambda \leq 1$, then $y = z = x$. Prove that the (n, k)-flat distributions are (the only) extremal points of C.

2. (Exercise on page I-3) Prove from scratch that every (n, k)-source is a convex combination of (n, k)-flat distributions.

3. (Exercise on page I-6) Recall from the lecture that one can define a bipartite multigraph $G_F(V_1, V_2, E)$ to every mapping $F : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, where $V_1 = \{0,1\}^n$, $V_2 = \{0,1\}^m$. In G_F, a pair of vertices $v_1 \in V_1$ and $v_2 \in V_2$ forms an edge, if and only if there exists $y \in \{0,1\}^d$ such that $F(v_1, y) = v_2$. Show that F is a (k, ϵ)-extractor if and only if G_F is a $(2^k, \epsilon)$-extractor graph.

4. A function $f : \{0,1\}^n \to \{0,1\}$ is (t, ϵ)-hard if for any circuit C of size at most t on n input variables,

$$\left| \mathbb{P}[C(x) = f(x)] - \frac{1}{2} \right| < \epsilon,$$

where x is distributed uniformly among all $\{0,1\}^n$ sequences, i.e., $x \sim U_n$. Show that there exists $(\epsilon^2 2^n/(3n), \epsilon)$-hard functions for every $0 < \epsilon < 1$, when n is sufficiently large. In particular, conclude that there exists $(t, \frac{1}{t})$-hard function, where $t := \left(\frac{2^n}{3n}\right)^{1/3}$.