Solutions 1

1. The solutions for the four items are as follows.

(i) Clearly $A \subseteq \mathrm{CH}(A)$, since every point $a \in A$ is a convex combination of itself. To prove that A is convex, let $x = \lambda_1 a_1 + \ldots + \lambda_k a_k \in \mathrm{CH}(A)$ and $y = \delta_1 b_1 + \ldots + \delta_l b_l \in \mathrm{CH}(A)$, where $a_1, \ldots, a_k, b_1, \ldots, b_l \in A$, the coefficients λ_i and δ_j are nonnegative and add up to one, i.e.,

$$\sum_{i=1}^{k} \lambda_i = \sum_{j=1}^{l} \delta_j = 1.$$

For each $0 \leq \lambda \leq 1$, we have

$$\begin{aligned} \lambda x + (1-\lambda) y = (\lambda\lambda_1) \cdot a_1 + \ldots + (\lambda\lambda_k) \cdot a_k \\ + ((1-\lambda)\delta_1) \cdot b_1 + \ldots + ((1-\lambda)\delta_l) \cdot b_l \end{aligned}$$

and since the sum of all the coefficients is

$$\sum_{i=1}^{k} \lambda\lambda_i + \sum_{j=1}^{l} (1-\lambda)\delta_j = \lambda \sum_{i=1}^{k} \lambda_i + (1-\lambda) \sum_{j=1}^{l} \delta_j = \lambda + (1-\lambda) = 1,$$

we clearly have $\lambda x + (1-\lambda) y \in \mathrm{CH}(A)$, thereby proving that $\mathrm{CH}(A)$ is convex.

(ii) To prove that $\mathrm{CH}(A)$ is the smallest convex set that contains A, it suffices to show that if B is convex and B contains A, then B contains all convex combinations of finite subsets of A. Equivalently, for every subset of k elements $\{a_1, \ldots, a_k\} \subseteq A$, and for every k nonnegative real numbers $\lambda_1, \ldots, \lambda_k$ adding up to one, the convex combination $\sum_{i=1}^{k} \lambda_i a_i$ belongs to B. We will prove this claim by induction on k. When $k = 1$ the claim is trivial. For the inductive step, we assume that B contains all convex combinations of at most $k-1$ elements from A. To prove that B contains all convex combinations of k elements, let $a_1, \ldots, a_k \in A$ and let $\lambda_1, \ldots, \lambda_k \geq 0$ be such that $\sum_{i=1}^{k} \lambda_i = 1$. If $\lambda_k = 0$, then the point $x = \sum_{i=1}^{k} \lambda_i a_i$ is actually a convex combination of $k-1$ elements from A, and by the inductive hypothesis, $x \in B$. Otherwise,

$$\begin{aligned} x = \sum_{i=1}^{k} \lambda_i a_i &= \sum_{i=1}^{k-1} \lambda_i a_i + \lambda_k a_k \\ &= (1-\lambda_k) \sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} a_i + \lambda_k a_k \end{aligned}$$

Since $\sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} = 1$, the point $y = \sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} a_i$ is a convex combination of $k-1$ points from A, hence belongs to B. Since B is convex and $a_k, y \in B$, we must have $x = (1-\lambda_k)y + \lambda_k a_k \in B$. By induction, the claim is true for all $k \geq 1$, finishing the proof.

(iii) Let P_1 and P_2 be two (n,k)-source probability distributions in C, i.e., $P_1(x), P_2(x) \leq 2^{-k}$ for all $x \in \{0,1\}^n$. Let $P = \lambda P_1 + (1-\lambda)P_2$, where $0 \leq \lambda \leq 1$. Then clearly

$$P(x) = \lambda P_1(x) + (1-\lambda)P_2(x) \leq \lambda \cdot 2^{-k} + (1-\lambda) \cdot 2^{-k} = 2^{-k},$$

therefore P is an (n,k)-source. This implies that C is convex, finishign the proof.

(iv) Let P be an (n,k)-flat probability distribution, and assume that $P = \lambda P_1 + (1-\lambda)P_2$, where $0 \leq \lambda \leq 1$ and $P_1, P_2 \in C$ are two (n,k)-source distributions. Let $A = \{x \in \{0,1\}^n : P(x) > 0\}$. We know that $|A| = 2^k$ and for each $x \in A$, we have

$$\begin{aligned} 2^{-k} = P(x) &= \lambda P_1(x) + (1-\lambda)P_2(x) \\ &\leq \lambda \cdot 2^{-k} + (1-\lambda) \cdot 2^{-k} \\ &= 2^{-k} \end{aligned}$$

hence, we must have $P_1(x) = P_2(x) = 2^{-k}$ for all $x \in A$, which implies that $P_1 = P_2 = P$, concluding the proof.

2. An (n,k)-source is a probability distribution $P : \{0,1\}^n \to [0,1]$ such that $P(x) \leq 2^{-k}$ for all $x \in \{0,1\}^n$. A (n,k)-flat source is a probability distribution $Q_A : \{0,1\}^n \to [0,1]$ such that either $Q(x) = 0$ if $x \notin A$ and $Q(x) = 2^{-k}$ when $x \in A$, where A is any subset of $\{0,1\}^n$ having size 2^k.

For any given (n,k)-source P, let B_P be the set of all $x \in \{0,1\}^n$ such that $P(x) = 2^{-k}$; and let S_P be the set of all $x \in \{0,1\}^n$ such that $P(x) > 0$. Clearly $|B_P| \leq 2^k \leq |S_P|$. We will prove by induction on $t_P := |S_P| - |B_P|$, that P is a convex combination of (n,k)-flat distributions.

The base case $t_P = 0$ is trivial, because P itself is (n,k)-flat. Let P be one (n,k)-source such that $t_P = t$. Let A be any subset of S_P containing B_P and having size 2^k. Let $P' : \{0,1\}^n \to [0,1]$ be defined as

$$P'(x) := (1+\epsilon) \cdot P(x) - \epsilon \cdot Q_A(x),$$

where $\epsilon := \min\{\epsilon_1, \epsilon_2\}$,

$$\epsilon_1 := \min\left\{ \frac{1}{2^k P(x)} - 1 : x \in S_P \setminus A \right\} > 0, \text{ and}$$

$$\epsilon_2 := \min\left\{ \frac{P(x)}{Q_A(x) - P(x)} : x \in A \setminus B_P \right\} > 0.$$

Siehe nächstes Blatt!

Clearly P' is a probability distribution, since $P'(x) \geq 0$ for all $x \in \{0,1\}^n$, as $\epsilon \leq \epsilon_2$. Furthermore, P' is a (n,k)-source, as $\epsilon \leq \epsilon_1$. But either $|B_{P'}| > |B_P|$ (if $\epsilon = \epsilon_1$), or $|S_{P'}| < |S_P|$ (if $\epsilon = \epsilon_2$), in particular, we always have $t_{P'} < t$. By the inductive hypothesis, P' is a convex combination of (n,k)-flat distributions. But

$$P(x) = \frac{1}{1+\epsilon} \cdot P'(x) + \frac{\epsilon}{1+\epsilon} \cdot Q_A(x),$$

therefore P is also a convex combination of (n,k)-flat distributions, finishing the proof by induction.

3. This exercise is about unravelling the definitions. A map $F : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k,ϵ)-extractor if for every (n,k)-source P, we have

$$\delta(F(P, U_d), U_m) < \epsilon,$$

where $\delta(P_1, P_2) := \max_{S \subseteq \{0,1\}^m} |P_1(S) - P_2(S)|$ is the statistical distance between two distributions P_1 and P_2. By the flat-source lemma, this definition is equivalent to the one where we replace the condition that P is a (n,k)-source with the condition that P is (n,k)-flat.

Using this version of the defintion, a map F is (k,ϵ)-extractor if for every set $A \subseteq \{0,1\}^n$ of size 2^k (here A represents the support of the (n,k)-flat distribution) and for every set $S \subseteq \{0,1\}^m$, we have

$$\left| \frac{|\{y \in \{0,1\}^d : \exists a \in A \text{ s.t. } F(a,y) \in S\}|}{2^{k+d}} - \frac{|S|}{2^m} \right| < \epsilon. \tag{1}$$

The bipartite multigraph $G_F = (V_1, V_2, E)$ with left degree 2^d is a $(2^k, \epsilon)$-extractor (multi)graph if for every $A \subseteq V_1$, having size $|A| = 2^k$ and any $S \subseteq V_2$, we have

$$\left| \frac{|E(A,S)|}{|E(A,V_2)|} - \frac{|S|}{|V_2|} \right| < \epsilon, \tag{2}$$

but $|E(A,S)| = |\{y \in \{0,1\}^d : \exists a \in A \text{ s.t. } F(a,y) \in S\}|$, $|E(A,V_2)| = 2^d|A| = 2^{k+d}$, and $|V_2| = 2^m$, hence the inequalities (1) and (2) are equivalent, concluding the solution of the exercise.

4. From the lecture notes (page I-11b), the number of Boolean circuits of size t (i.e., having t gates), is bounded above by $2^t(2n+t-1)^{2t}$. For a fixed Boolean circuit $C : \{0,1\}^n \to \{0,1\}$ of size t, if we choose a function $f : \{0,1\}^n \to \{0,1\}$ uniformly

Bitte wenden!

at random, and denote by Y_x the indicator of the event $f(x) = C(x)$, then $Y := \sum_{x\in\{0,1\}^n} Y_x \sim \text{Bin}(2^n, \frac{1}{2})$. By the Chernoff-Hoeffding's bound, we know that

$$\mathbb{P}[|Y - 2^{n-1}| > \epsilon \cdot 2^n] \leq 2e^{-2\epsilon^2 2^n}.$$

Thus, by the union bound, the probability that f is not (t, ϵ)-hard is bounded above by

$$\begin{aligned} 2^{t+1}(2n + t - 1)^{2t} e^{-2\epsilon^2 2^n} &= \exp((t + 1) \ln 2 + 2t \ln(2n + t - 1) - 2\epsilon^2 2^n) \\ &\leq \exp(2t \ln 2 + 3t \ln(t) - 2\epsilon^2 2^n) \\ &\leq \exp(3nt - 2\epsilon^2 2^n) = \exp(-\epsilon^2 2^n), \end{aligned}$$

but $\exp(-\epsilon^2 2^n) < 1$, therefore there exists $(\epsilon^2 2^n/(3n), \epsilon)$-hard functions for every $0 < \epsilon < 1$.