CS 744: Pseudorandom Generators
Assignment 1

Deadline: February 10, 2016

General Instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly encouraged to solve the problems by yourself. You may discuss but write the solutions on your own. Any copying will get zero in the whole assignment.
- Please submit the answers in soft-copy form (as a single pdf file) via email to diptarka@cse.iitk.ac.in. Scanned copy of any handwritten answer will not be allowed. Delay in submission will cause deduction in marks.

In this assignment we assume that all of you already know the basic definitions and results related to circuit model (notion of non-uniformity) and the complexity class BPP. If you do not know, then consult any standard book on complexity theory.

In this assignment any distribution denoted by subscript $n \in \mathbb{N}$ (e.g., D_n) is a distribution over $\{0,1\}^n$. Here we consider asymptotic version of the definitions of distinguishability and pseudorandomness covered (or going to be covered) in the class. Let us first tell you what do we mean by the asymptotic version of the definition of distinguishability.

Definition 1 (Distinguishability)**.** *Two ensembles of distributions $D = \{D_n\}_{n\in\mathbb{N}}$ and $D = \{D'_n\}_{n\in\mathbb{N}}$ are* distinguishable by class $\mathcal{C}$ *if there exists a function $f : \{0,1\}^* \to \{0,1\}$ which belongs to the class $\mathcal{C}$ such that for some polynomial $p(n)$, for large enough n, the following holds*

$$|Pr[f(D_n) = 1] - Pr[f(D'_n) = 1]| \geq \frac{1}{p(n)}.$$

Now we can naturally define pseudorandomness by the following definition.

Definition 2 (Pseudorandomness)**.** *An ensemble of distributions $D = \{D_n\}_{n\in\mathbb{N}}$ is said to be* pseudorandom with respect to a class $\mathcal{C}$ *if it can not be distinguished by class $\mathcal{C}$ from the ensemble of uniform distributions, denoted as $U = \{U_n\}_{n\in\mathbb{N}}$.*

Question 1: [8+2] Consider any function $s(n) \geq \omega(\log n)$.

(a) Show that there exists an ensemble of distributions $D = \{D_n\}_{n\in\mathbb{N}}$ which is pseudorandom with respect to the class of all polynomial-size non-uniform circuits, where D_n has support size[1] $2^{s(n)}$.

[Hint: For a fixed n, choose $2^{s(n)}$ random strings independently and assign uniform probability over the chosen strings. Use Chernoff bound to argue that with non-zero probability this process will generate desired pseudorandom distribution ensemble.]

(b) Also show that this $\omega(\log n)$ bound on $s(n)$ is actually tight.

Question 2: [10] Let us now modify the definition of distinguishability slightly by allowing functions of the form $f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ that belong to the class $\mathcal{C}$. We call two ensembles of distributions $D = \{D_n\}_{n\in\mathbb{N}}$ and $D = \{D'_n\}_{n\in\mathbb{N}}$ are *distinguishable via auxiliary input by class* $\mathcal{C}$ if there exists a function $f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ which belongs to the class $\mathcal{C}$ such that for some polynomial $p(n)$ and $r(n)$, for large enough n, there exists a $z_n \in \{0,1\}^{r(n)}$ which satisfies the following

$$|Pr[f(D_n, z_n) = 1] - Pr[f(D'_n, z_n) = 1]| \geq \frac{1}{p(n)}.$$

Now consider the following two notions:

(i) distinguishability by the class of polynomial-size non-uniform circuits, and

(ii) distinguishability via auxiliary input by the class of all probabilistic polynomial-time algorithms.

Which one of the above two is more powerful, i.e., whether $(i) \implies (ii)$ or $(ii) \implies (i)$? Give proper justification behind your answer.

Question 3: [3+7] Now let us talk about distributions that not only can not be distinguished from uniform distribution, but behave exactly same as uniform distribution, i.e., for $f : \{0,1\}^* \to \{0,1\}$ belongs to some class $\mathcal{C}$, for ever $n \in \mathbb{N}$, the following holds

$$Pr[f(D_n) = 1] = Pr[f(U_n) = 1].$$

(a) Suppose you have a halting probabilistic Turing machine M. Now for a fixed $n \in \mathbb{N}$, use averaging argument to show that you can find two strings $x, y \in \{0,1\}^n$ such that for a distribution D_n which incurs non-zero probability only on x and y,

$$Pr[M(D_n) = 1] = Pr[M(U_n) = 1].$$

(b) Now consider any non-decreasing and unbounded function $k : \mathbb{N} \to \mathbb{N}$ and for a fixed $n \in \mathbb{N}$, set of first $k(n)$ halting probabilistic Turing machines appeared in standard enumeration and denote this set by $\mathcal{M}$. Now generalize the above argument and use a little bit of basic linear algebra to show that for every $n \in \mathbb{N}$ you can construct distributions D_n of support size only $k(n) + 1$ such that for every $M \in \mathcal{M}$,

$$Pr[M(D_n) = 1] = Pr[M(U_n) = 1].$$

[Hint: For every $x \in \{0,1\}^n$, define a suitable $k(n)$ dimensional vector over $\mathbb{R}$.]

[1] Number of strings having non-zero probability according to the distribution D_n

Question 4: [5+10+5] Consider the following game: Alice picks any $a \in A$ and Bob picks any $b \in B$ and depending on their choices, Alice gains an amount of $g(a, b)$ whereas Bob gains $-g(a, b)$, for some function $g : A \times B \to \mathbb{R}$. Now suppose $\mathcal{A}$ and $\mathcal{B}$ denote the set of all distributions over A and B respectively. Then by a celebrated result of Yao, we know that

$$\max_{\hat{\mathrm{A}} \in \mathcal{A}} \min_{b \in B} \mathbb{E}_{a \sim \hat{\mathrm{A}}}[g(a, b)] = \min_{\hat{\mathrm{B}} \in \mathcal{B}} \max_{a \in A} \mathbb{E}_{b \sim \hat{\mathrm{B}}}[g(a, b)].$$

(a) Now consider the set of ensembles of distributions which are distinguishable from each other by the class of all polynomial-size non-uniform circuits and let us denote this set by $\mathcal{D}$. Try to construct a game similar as mentioned above, to show that there exists a family of probabilistic circuits (circuits which can also flip coins) $\{C_n\}_{n \in \mathbb{N}}$ such that for some polynomial $p(n)$, for any two ensembles of distributions $D = \{D_n\}_{n \in \mathbb{N}}$ and $D = \{D'_n\}_{n \in \mathbb{N}}$ belong to $\mathcal{D}$, the following holds for sufficiently large n,

$$|Pr[C_n(D_n) = 1] - Pr[C_n(D'_n) = 1]| \geq \frac{1}{p(n)}.$$

(b) Note that above circuit family $\{C_n\}_{n \in \mathbb{N}}$ may not be of polynomial-size. Now view each probabilistic circuit as distribution of circuits and then draw a few (specify how many!) samples according to that distributions and take average of them.

Show that in the above process you will get some polynomial-size circuit family $\{C'_n\}_{n \in \mathbb{N}}$ such that for some polynomial $q(n)$, for any two ensembles of distributions $D = \{D_n\}_{n \in \mathbb{N}}$ and $D = \{D'_n\}_{n \in \mathbb{N}}$ belong to $\mathcal{D}$, the following holds for sufficiently large n,

$$|Pr[C'_n(D_n) = 1] - Pr[C'_n(D'_n) = 1]| \geq \frac{1}{q(n)}.$$

In summary, if you want to comment on whether two ensembles D and D' are distinguishable or not by the class of polynomial-size non-uniform circuits, it is sufficient to consider only one polynomial-size circuit family $\{C'_n\}_{n \in \mathbb{N}}$ instead of all family of polynomial-size circuits.

(c) Argue whether the above technique will work or not if we consider the class of probabilistic polynomial-time algorithms instead of the family of polynomial-size circuits.