Problem Set 3

Pseudorandomness, Autumn 2023, University of Chicago
Instructor: William Hoza (williamhoza@uchicago.edu)

Submission. Solutions are due **Wednesday, November 8** at 5pm Central time. Submit your solutions through Canvas. You are encouraged to typeset your solutions in LaTeX. (Consider using Overleaf, a popular online LaTeX editor.) If you prefer, you may submit a photo of handwritten solutions instead.

The collaboration and resource policies below can also be found on the course webpage.

Collaboration. You are encouraged to collaborate with your classmates on problem sets, but you must adhere to the following rules.

- Before discussing a problem with a classmate, you must work on the problem on your own for at least 20 minutes.
- You must ultimately write your solution on your own. While writing your solution, you may not consult any notes that you took during a discussion with another classmate.
- In your write-up, you must list any classmates who contributed to your solution through discussion. The fact that A contributed to B's solution does not necessarily mean that B contributed to A's solution.

Permitted Resources for Full Credit. Beyond discussions with me and discussions with classmates as discussed above, you may use the course texts and any notes that might be posted in the "Course Timeline" section of the course webpage. If you wish to receive full credit on a problem, you may not use any other resources.

Permitted Resources for Partial Credit. If you wish, you may use outside resources (Wikipedia, ChatGPT, Stack Exchange, research papers, etc.) to solve a problem for partial credit. If you decide to go this route, you must make a note of which outside resources you used when you were working on each problem. You must disclose using a resource even if it was ultimately unhelpful for solving the problem. Furthermore, if you consult an outside resource while working on a problem, then you must not discuss that problem with your classmates.

Problem 1 (15 points)**.** Let G be an ε-spectral expander on N vertices.

(a) Show that the diameter of G is at most $\left\lceil \frac{\log N}{\log(1/\varepsilon)} \right\rceil$. *Note:* This implies as a special case that if $\varepsilon \leq 1/N$, then every vertex in G is adjacent to every other vertex. We have used this fact in class multiple times. However, for this problem, you may *not* take this fact as given. Instead, you should solve the problem "from scratch."

(b) Let S be an independent set of vertices, i.e., no two vertices in S are connected by an edge. Show that

$$|S| \leq \frac{\varepsilon}{1+\varepsilon} \cdot N.$$

Hint: Use Theorem 4.6 in Vadhan's text.

(c) Let $\phi\colon [N] \to [k]$ be a k-coloring of G, i.e., if s and t are joined by an edge, then $\phi(s) \neq \phi(t)$. Show that

$$k \geq \frac{1+\varepsilon}{\varepsilon}.$$

Definition 1 (Robust PRGs)**.** Let $\mathcal{F}$ be a class of functions $f\colon \{0,1\}^n \to \mathbb{R}$ and let $\varepsilon, \delta > 0$. A *δ-robust ε-PRG* for $\mathcal{F}$ is a function $G\colon \{0,1\}^{s_1} \times \{0,1\}^{s_2} \to \{0,1\}^n$ such that for every $f \in \mathcal{F}$,

$$\Pr_{x \sim U_{s_1}} \left[\left| \mathop{\mathbb{E}}_{y \sim U_{s_2}} [f(G(x,y))] - \mathbb{E}[f] \right| \leq \varepsilon \right] \geq 1 - \delta.$$

The parameter s_1 is called the *outer seed length* of G, and s_2 is called the *inner seed length*.

In this problem, you will show that every PRG can be converted into a robust PRG with an extremely small inner seed.

Problem 2 (10 points)**.** Let $n, s \in \mathbb{N}$, let $\mathcal{F}$ be a class of functions $f\colon \{0,1\}^n \to \{0,1\}$, and let $\varepsilon > 0$. Assume that there exists an explicit ε-PRG for $\mathcal{F}$ with seed length s. Show that for every $\delta > 0$, there exists an explicit δ-robust (2ε)-PRG for $\mathcal{F}$ with outer seed length $O(s + \log(1/\delta))$ and inner seed length $O(\log(s/\varepsilon) + \log\log(1/\delta))$.

You may take as given the following theorem, which we state but do not prove in class.

Theorem 1 (GUV Extractor)**.** *For every $\ell, k \in \mathbb{N}$ with $k \leq \ell$, for every $\varepsilon > 0$, there exists an explicit (k,ε)-extractor $\mathsf{Ext}\colon \{0,1\}^\ell \times \{0,1\}^d \to \{0,1\}^m$ with seed length $d = O(\log(\ell/\varepsilon))$ and output length $m \geq k/2$.*

Hint: In class, we show that every (k,ε)-extractor $\mathsf{Ext}\colon \{0,1\}^\ell \times \{0,1\}^d \to \{0,1\}^m$ induces an (ε,δ)-sampler for functions on m bits, where $\delta = 2^{k-\ell+1}$.
