Problem Set 3

- Due Date: **22 Nov 2021**
- The points for each problem is indicated on the side. This problem set has **60** points but you may solve any **45** points worth of questions among these for a full score (the remaining **15** points are bonus). Any additional points obtained will still count towards your final aggregate.
- Turn in your problem sets electronically (PDF; either LaTeXed or scanned etc.) on Acadly.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring to sources other than the text book and class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources in your writeup, with a brief remark on *why* you sought that source. This **will not** affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- Be clear in your writing.

1. **[Cryptographic PRGs]** (2 + 3 + 7 + 8)

   In the cryptographic setting, we often consider PRGs of the form $G : \{0,1\}^s \to \{0,1\}^{2s}$ (for example) for the class of all poly(s)-sized circuit with $\varepsilon = 1/s^{\omega(1)}$, even while assuming that the function G itself is polynomial time computable! That is, G is an efficient PRG that is secure against potentially more powerful adversaries than needed to compute G.

   We'll refer to such PRGs as *cryptographically secure* PRGs.

   (a) A PRG $G : \{0,1\}^s \to \{0,1\}^m$ is said to be a *seed-revealable PRG* if even G' given by $G'(s) = (s, G(s))$ is a PRG. That is, G remains a PRG even if the seed s is "revealed".
   Show that there cannot be any cryptographically secure PRG that is also seed-revealable.

   (b) If $G : \{0,1\}^s \to \{0,1\}^m$ is a cryptographically secure PRG, then prove that $G' : \{0,1\}^{\ell+s} \to \{0,1\}^{\ell+m}$ given by $G(s_1, s_2) = s_1 \cdot G(s_2)$ (where $s_1 \in \{0,1\}^\ell$) is also a cryptographically secure PRG.

   (c) If $G : \{0,1\}^s \to \{0,1\}^{2s}$ is a cryptographically secure PRG, show that the function $H : \{0,1\}^s \to \{0,1\}^{3s}$ given by $H(s) = x \cdot u \cdot v$ where $G(s) = x \cdot y$ and $G(y) = u \cdot v$ is also cryptographically secure.
   What about $H' : \{0,1\}^s \to \{0,1\}^{4s}$ given by $H'(s) = x \cdot y \cdot u \cdot v$? Is it a PRG as well? Justify your answer.

   (d) Suppose $G : \{0,1\}^s \to \{0,1\}^{2s}$ is a cryptographically secure PRG. Here are two candidate cryptographically secure PRGs of the form $\{0,1\}^s \to \{0,1\}^{3s}$:

   $$H_1(s) := (x \oplus y) \cdot u \cdot v$$
   $$H_2(s) := x \cdot (y \oplus u) \cdot v$$

Base version: (2021-11-08 09:33:05 +0530) , dbbefa8

where $G(s) = x \cdot y$ and $G(y) = u \cdot v$.

Turns out, one of the above two candidates is provably always a cryptographically secure PRG (that is, H_b is cryptographically secure PRG whenever G is cryptographically secure), and the other is not (that is, there is a cryptographically secure G for which $H_{b'}$ is provably NOT secure). Find out which is which, and justify your answer with either a proof or a distinguisher.

[Hint: Try and use some of the previous parts of this question. It might help to keep in mind that for any fixed y, the distribution of $r \oplus y$ is uniform if r is chosen uniformly at random.]

2. **[PRGs for 2-step communication c protocols using hash functions]** $(2 + 3 + 5 + 5)$

Let $\Sigma = \{0,1\}^n$ and $\mathcal{H} = \{h \colon \Sigma \to \Sigma\}$ be a pairwise independent hash family. In this question, you will show that for every $A, B \subseteq \Sigma$ we have

$$\Pr_{h \in \mathcal{H}} \left[\left| \Pr_{x \in \Sigma}[x \in A \ , \ h(x) \in B] - \mu(A)\mu(B) \right| \geq \varepsilon \right] \ \leq \ \frac{1}{\varepsilon^2 |\Sigma|}, \tag{1}$$

where $\mu(A), \mu(B)$ refers to $\frac{|A|}{|\Sigma|}$ and $\frac{|B|}{|\Sigma|}$ respectively.

(a) For any $x \in A$, let $I_x = \mathbb{1}_{h(x) \in B}$, the indicator random variable for whether $h(x) \in B$. Let $Y = \sum_{x \in A} I_x$.
Show that $\frac{1}{|\Sigma|} \cdot \mathbb{E}[Y] = \mu(A)\mu(B)$.

(b) Show that $\mathrm{Var}(Y) \leq \mathbb{E}[Y]$.

(c) Show that $\Pr\left[\left| \frac{1}{|\Sigma|} \cdot Y - \alpha\beta \right| > \varepsilon \right] \leq \frac{\alpha\beta}{\varepsilon^2 |\Sigma|}$, and conclude (1).

(d) By suitably instantiating ε in the above part, infer from the above that the following map:

$$G : (x, h) \mapsto (x, h(x))$$

is an ε-PRG for 2-step communication-c algorithms for any constant $\varepsilon > 0$ and $c = O(\log n)$.

3. **[Basic properties of the matrix max-norm]** (7)

In class, we used the following norm on matrices:

$$\|M\| := \max_{i \in [n]} \left(\sum_{j \in [m]} |M_{i,j}| \right),$$

if M is an $n \times m$ matrix.

Prove that $\|A + B\| \leq \|A\| + \|B\|$ and $\|AB\| \leq \|A\| \cdot \|B\|$.

4. **[Explicit constructions of combinatorial designs]** (8)

Let us assume that k, ℓ are powers of 2, with $k \leq \ell^2$. Let $\mathbb{F}$ be the finite field of size ℓ/k and let S be a set of k distinct elements from $\mathbb{F}$. For any $a \leq k$, define the following family of sets

$$\mathcal{D} = \{T_p \ : \ p \in \mathbb{F}[x] \ , \ \deg(p) < a\}$$

where $T_p = \{(a, p(a)) \ : \ a \in S\}$.

That is, there is a set T_p for every univariate polynomial $p(x) \in \mathbb{F}[x]$ of degree at most a, where the set is the "graph" of the polynomial.

Show that the $\mathcal{D}$ is an (ℓ, a)-combinatorial design of size $\left(\frac{\ell}{k}\right)^a$. That is, $\mathcal{D}$ is a collection of $\left(\frac{\ell}{k}\right)^a$ sets of size exactly k whose pairwise intersection of size less than a.

5. **[PRGs imply hard functions]** (10)

Suppose that for every m, there exists a mildly explicit $\frac{1}{m}$-PRG $G_m : \{0,1\}^{d(m)} \to \{0,1\}^m$ against size-m circuits.

Show that there is a function $f_\ell : \{0,1\}^\ell \to \{0,1\}$ that is computable in time $2^{O(\ell)}$ that cannot be computed by circuits of size $t(\ell) = \Omega(d^{-1}(\ell - 1))$. In particular, if $d(m) = \log m$, then we have a $2^{\Omega(\ell)}$ lower bound for f_ℓ.

[Hint: Consider the function that checks if there is a $y \in \{0,1\}^{d(m)}$ such that $G_m(y)$ begins with 101001.]