CS747 - RANDOMIZED METHODS IN COMPUTATIONAL COMPLEXITY
NITIN SAXENA

END-SEMESTER EXAMINATION (2023-24/I)

POINTS: 40

DATE GIVEN: 21-NOV'23 DUE: 24-NOV'23 (8PM)

Rules:

- You are *not* allowed to discuss.
- Write the solutions on your own and honorably *acknowledge* the sources if any. `http://cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Submit your solutions, before time, to your TA. Please give your LaTeXed or Word processed solution-sheet in PDF. This will be graded, and commented, in-place.
- Clearly express the fundamental *idea* of your proof/ algorithm before going into the other proof details. The distribution of partial marks is according to the proof steps.
- There will be a penalty if you write unnecessary or unrelated details in your solution. Also, do not repeat the proof details covered before.

Question 1: *[10 points]* Suppose boolean function f is in E with $\mathrm{H}_{\mathrm{avg}}(f) \geq n^4$. Then, the function $g : z_1 z_2 \mapsto z_1 \circ z_2 \circ f(z_1) \circ f(z_2)$, for $z_1, z_2 \in \{0,1\}^{\ell/2}$, is an $(\ell+2)$-prg.

Question 2: *[12 points]* An ecc $E : \{0,1\}^n \to \{0,1\}^m$ is called *ϵ-biased* if for all nonzero $x \in \{0,1\}^n$, $\#\{i \mid E(x)_i \neq 0\}/m \in \left(\frac{1}{2} - \epsilon, \frac{1}{2} + \epsilon\right)$.

For every $\epsilon \in \left(0, \frac{1}{2}\right)$, prove the existence of an *ϵ-biased linear* error-correcting code $E : \{0,1\}^n \to \{0,1\}^{\mathrm{poly}(n/\epsilon)}$ with poly-time encoding and decoding algorithms.

Let us explore some fundamental concepts from cryptography.

Function $f : \{0,1\}^* \to \{0,1\}^*$ is called *one-way* if

- f is poly-time computable, and
- for all randomized poly-time algorithms A, $\forall c > 0$, for all sufficiently large n,

$$\text{Prob}\left[A(f(x), 1^n) \in f^{-1}(f(x))\right] \;<\; n^{-c},$$

where the probability is over $x \in \{0,1\}^n$ and the random bits of A.

Predicate $b : \{0,1\}^* \to \{0,1\}$ is called *hard-core of a function* f if

- f, b are poly-time computable, and
- for all randomized poly-time algorithms A, $\forall c > 0$, for all sufficiently large n,

$$\text{Prob}\left[A(f(x)) = b(x)\right] \;<\; \frac{1}{2} + n^{-c},$$

where the probability is over $x \in \{0,1\}^n$ and the random bits of A.

Question 3: *[4+4+4+6 points]* Prove the following facts:

(1) If there is a one-way function then there is a *length-preserving* one-way function.

(2) If b is hard-core (of some f) then (for the *uniform* distribution U_n),

$$|\,\text{Prob}\left[b(U_n) = 0\right] \;-\; \text{Prob}\left[b(U_n) = 1\right]\,| \;=\; n^{-\omega(1)}.$$

(3) If b is hard-core of some one-to-one function f, then f is one-way.

(4) For every one-way function there is a hard-core predicate.

□□□