Pseudorandomness	**Fall 2023/4**

Problem Set 2

Publish Date: February 13, 2024 — Due Date: March 5, 2024 (all day long)

Note. Submissions must be made in pairs. Please type your solutions and submit them as a PDF file through Moodle. If you have any questions, feel free to send an email to Itay or to Gil.

Question 1. In class, we examined a third method for constructing a family of expander graphs, based on the Zig-Zag product, as detailed in the penultimate slide of the presentation, as given by

$$G_1 = H^2,$$
$$G_{t+1} = (G_{\lceil t/2 \rceil} \otimes G_{\lfloor t/2 \rfloor})^2 \, ⓩ \, H.$$

In this question you are asked to choose the parameters of H so to obtain an infinite family of d-regular graphs and analyze the parameters of this construction, covering the degree, spectral expansion, and sizes of the graphs generated by this family.

Question 2. For proving $\mathbf{SL} = \mathbf{L}$ we used the fact that for an undirected connected graph $G = (V, E)$ on n vertices, which is not bipartite, $\gamma(G) \geq \frac{1}{n^c}$ for some universal constant c. In this question you will prove this bound. To this end, explain first why is it suffices to prove the statement for regular graphs, and then proceed by solving the following questions for a regular G:

1. Prove that
$$\omega_2(G) = \max_{\substack{\psi \perp \mathbf{1} \\ \|\psi\|=1}} \psi^\mathsf{T} \mathbf{W} \psi,$$
where $\mathbf{W}$ is the random walk matrix of G, and $\mathbf{1}$ is the all-ones vector.

2. Prove that
$$\omega_n(G) = \min_{\|\psi\|=1} \psi^\mathsf{T} \mathbf{W} \psi.$$

3. With these, complete the proof. *Hint:* When faced with an expression of the form $\sum_{uv \in E} \psi(u)\psi(v)$, it would be useful to complete it to a square, namely, expressing it as a linear combination of $\sum_{uv \in E} (\psi(u) - \psi(v))^2$ and some other friendly expressions.

Question 3. In this question you will prove a strong relation, equivalence really, between small-bias sets and Cayley graphs. Let $S \subseteq \{0,1\}^n$. Prove that S is an ε-biased set if and only if the Cayley graph $\mathsf{Cay}(\{0,1\}^n, S)$ is an ε-spectral expander.

Question 4. Give an explicit construction of an ε-biased set $S \subseteq \{0,1\}^n$ of size $\widetilde{O}(\frac{n}{\varepsilon^3})$ (where, recall, $\widetilde{O}(\cdot)$ hides poly-logarithmic factors). *Hint:* Consider the powering construction we saw in class and think how you can replace the truly uniform element y with some other pseudorandom string.

Question 5. In this question you will construct yet another ε-biased set $S \subseteq \{0,1\}^n$. For a suitable choice of a prime p, the elements of your (multi-)set will be indexed by $\mathbb{F}_p$. For $x \in \mathbb{F}_p$, the string $s_x \in S$ is defined as follows: For $i \in [n]$, $s_x(i) = \chi(x+i)$, where χ is the quadratic residue character. Analyze the construction and figure out what is the size of S in terms of n and ε (for a suitable choice of p).

Question 6. This question is about space-bounded computation.

1. You are given as input a number $a \in [0,1)$ which is encoded using b-bits in the natural way (e.g., for $b=2$, the four possible memory contents 00, 01, 10, 11 correspond to the numbers $a = 0, \frac{1}{4}, \frac{1}{2}$ and $a = \frac{3}{4}$, respectively). You are further given as input a natural number n and a number $\varepsilon \in (0,1)$. Devise a space-efficient algorithm for approximating a^n, where the approximation guarantee is ε. That is, the number your algorithm outputs, $\widetilde{a^n}$, should satisfy $|a^n - \widetilde{a^n}| \leq \varepsilon$. Analyze the space complexity of your algorithm.

2. We will now solve the same question but for matrices. You are given a $w \times w$ real matrix A, where every entry is in $[0,1)$ and is represented using b-bits of precision as before. You are further given n, ε as above, as well as indices $i,j \in [w]$. Devise a space-efficient algorithm which ε-approximates $(A^n)_{i,j}$. That is, your algorithm should output a number $\widetilde{(A^n)}_{i,j}$ satisfying $|\widetilde{(A^n)}_{i,j} - (A^n)_{i,j}| \leq \varepsilon$. Analyze the space complexity of your algorithm.