Pseudorandomness **Fall 2023/4**

Problem Set 3

Publish Date: March 10, 2024 Due Date: March 31, 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. Consider a generalized type of decision trees. In this variation, instead of labeling each node with a single variable, we label it with a subset of variables. The tree then branches left or right based on the parity of the values in this subset. Your task is to give an explicit construction a PRG for this model. Aim for the construction to be as efficient as possible in terms of seed length, considering the tree's size, denoted by m, the error ε, and the total number of variables, n.

Question 2. Let $G = (V, E)$ be a d-regular graph with rotation map $\pi_G : V \times [d] \to V \times [d]$. Assume that π_G satisfies the following property: For every $v \in V$ and $i \in [d]$, it holds that $\pi_G(v, i) = (u, i)$ for some $u \in V$ (informally, if v consider u as its i-th neighbor than so does u consider v as its i-th neighbor). Prove that in such case, for every graph H on d vertices, the spectrum of $G \circledz H$ contains that of H^2.

Question 3. Generalize the merger construction we saw in class to the case of $t \geq 2$ random variables. More precisely, given $\alpha, \varepsilon \in (0, 1)$, devise an efficient algorithm

$$\mathsf{Merg} : \left(\{0,1\}^n\right)^t \times \{0,1\}^d \to \{0,1\}^n$$

with the following property: For every sequence of random variables $X_1, \ldots, X_t$, supported on $\{0, 1\}^n$, if one of the X_i-s is uniform then

$$\mathsf{Merg}(X_1, \ldots, X_t, S) \approx_\varepsilon G,$$

where S is uniform over $\{0, 1\}^d$ and independent of the joint distribution of the X_j-s, and G has min-entropy $(1 - \alpha)n$. Your seed length should be $d = O\left(\frac{1}{\alpha} \log \frac{nt}{\varepsilon}\right)$. *Hint:* Instead of passing a line through points corresponding to $X_1, \ldots, X_t$, consider a higher degree curve.