Pseudorandomness **Fall 2023/4**

Problem Set 1

Publish Date: January 18, 2021 Due Date: February 8, 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 Gil.

Question 1. Define a set $R \subseteq \mathbb{F}_2^n$ as δ-*rigid* if, for every subspace $V \subseteq \mathbb{F}_2^n$ with dimension $\frac{n}{2}$, there exists at least one element $r \in R$ that is at a distance of at least δn from all elements of V. Prove that for a sufficiently small constant $\delta > 0$, a δ-rigid set of size $O(n)$ exists.

Question 2. Describe the process of deriving an infinite family of asymptotically-good binary error-correcting codes from a tree code which has a non-vanishing distance and a constant number of colors.

Question 3. Consider a connected, undirected graph $G = (V, E)$. If the adjacency matrix corresponding to G has m distinct eigenvalues, show that the diameter of G is strictly less than m. Hint: Think about the minimal polynomial of the adjacency matrix.

Question 4. Prove the expander mixing lemma. This lemma asserts that for any d-regular graph $G = (V, E)$ with n vertices and for every pair of vertex sets $S, T \subseteq V$ having densities $\alpha = \frac{|S|}{n}$ and $\beta = \frac{|T|}{n}$, respectively, the following inequality holds:

$$\left| \frac{|E(S,T)|}{nd} - \alpha\beta \right| \leq \omega(G)\sqrt{\alpha(1-\alpha)\beta(1-\beta)}.$$

Question 5. Given a prime number p, consider the Cayley graph G on the vertex set $\mathbb{Z}_p^3$ with the set of generators $S = \{(b, ab, a^2b) \mid a, b \in \mathbb{Z}_p\}$. What is the value of $\omega(G)$?