

Problem 1 (fooling width-2 ROBPs) [5 pts]. Currently we don't know how to construct RPGs against ROBPs with seed length $o(\log^2 n)$, even when the width w is a constant. Notice that in this case we cannot use the assumption that the ROBP is time independent, as it will increase the width by a factor of n . In this problem we will examine the simplest non-trivial case where $w = 2$.

1. [2 pt]. Let $\wedge$ be the binary operation on $\{\pm 1\}$ that represents the AND function, i.e.

$$x \wedge y = \begin{cases} 1 & \text{if } x = y = 1 \\ -1 & \text{if } x = -1 \text{ or } y = -1. \end{cases}$$

Let $g: \{\pm 1\}^n \rightarrow \{\pm 1\}$, and define $f: \{\pm 1\}^n \rightarrow \{\pm 1\}$ as

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_n) \wedge x_n.$$

Prove the following inequality on the Fourier spectra of f and g :

$$\sum_{S \subseteq [n]} |\widehat{f}(S)| \leq 1 + \sum_{S \subseteq [n]} |\widehat{g}(S)|.$$

Hint. Write $\wedge$ as a polynomial and use linearity of the Fourier transform.

2. [2 pt]. Let B be a length- n , width-2 ROBP. Consider a change of domain on B , by changing the labels on the edges and output nodes of B from $\{0, 1\}$ to $\{\pm 1\}$. Moreover, in every layer of B we also label the two nodes, one with 1 and the other with -1 .

Define $f_t: \{\pm 1\}^n \rightarrow \{\pm 1\}$ so that $f_t(x_1, \dots, x_n)$ is the label on the node in layer- $(t + 1)$ reached by following the edges labeled with $x_1, \dots, x_t$ from the initial node. For instance, f_0 is a constant function, and f_n is exactly the function computed by B . Prove that for every $t = 1, \dots, n$,

$$\sum_{S \subseteq [n]} |\widehat{f_t}(S)| \leq 1 + \sum_{S \subseteq [n]} |\widehat{f_{t-1}}(S)|.$$

Hint. Observe that f_t is a function of f_{t-1} and x_t . How many such functions are there? Can you classify them?

3. [1 pt]. Conclude that there exists explicitly constructed PRG $G: \{0, 1\}^\ell \rightarrow \{\pm 1\}^n$ that ε -fools every length- n , width-2 ROBP, with $\varepsilon = 0.1$ and seed length $\ell = O(\log n)$.

Hint. We have learned about the construction, which has a fooling criteria based on the Fourier spectrum of the distinguisher.

Problem 2 (graph theoretic properties of expanders) [5 pts]. Besides vertex and edge expansion, there are a lot more graph theoretic properties that an expander shares with a random graph. Here we explore some of the most important ones.

In all questions below, $H = (V, E)$ is a simple degree- d regular graph on $|V| = n$ vertices with constant spectral expansion $\gamma = 1 - \lambda > 0$.

1. **[2 pt].** (Rapid mixing.) Let $v_0, v_1, \dots, v_t$ be a random walk on H from a fixed starting vertex v_0 . Show that the total variation distance between the distribution of v_t and the uniform distribution over V is at most ε for some $t = O(\log(n/\varepsilon))$.

Hint. Let A be the adjacency matrix of H . Then one step of a random walk on H corresponds to multiplying the stochastic matrix $\frac{1}{d}A$. Use the definition of spectral expansion.

2. **[1 pt].** (Low diameter.) Prove that the diameter of H (the longest distance between any two vertices) is at most $O(\log n)$.

Hint. Two vertices v, w has distance at most t if the random walk from v of length t reaches w with non-zero probability. Alternatively, you can also prove this fact using vertex expansion.

3. **[1 pt].** (Independent set, vertex cover and chromatic number.) Prove that:

- Every independent set of H has size at most $\frac{\lambda n}{1+\lambda}$.
- Every vertex cover of H has size at least $\frac{n}{1+\lambda}$.
- The chromatic number of H is at least $1 + \lambda^{-1}$.

Hint. Use the strongest form of the expander mixing lemma.

4. **[1 pt].** (Far from 3-colorable.) From the last question we know that when $\lambda < 1/2$ (or $\gamma > 1/2$), the graph H is already not 3-colorable. Show that H is actually far from being 3-colorable; that is, given any 3-coloring $c : V \rightarrow \{1, 2, 3\}$, for a uniformly random edge $(v, w) \in E$ we have

$$\Pr_{(v,w) \sim E} [c(v) = c(w)] \geq \frac{1}{3}(1 - 2\lambda).$$

Hint. Similar to the last question, but instead of the number of edges within each set of vertices with the same color being zero, you need to lower bound the number of such edges.